STANDARD AGREEMENT **CalHR# «New_Contract_Number»**

STD 213 (Rev 06/03)

AGREEMENT NUMBER
REGISTRATION NUMBER

1. This Agreement is entered into between the State Agency and the Contractor named below:

STATE AGENCY'S NAME

CONTRACTOR'S NAME

Department of Human Resources

2. The term of this Agreement is: 07/01/2015 through 06/30/2016

3. The maximum amount of this Agreement is: **$**

4. The parties agree to comply with the terms and conditions of the following exhibits which are by this reference made a part of the Agreement.

Exhibit A – Scope of Work	2 pages
Attachment 1, Statement of Work	6 pages
Attachment 2, Deduction Codes	1 page
Attachment 3, File Requirements	4 pages
Attachment 4, Sample Contribution Time Table	3 pages
Attachment 5, California Administrative Code Title 2, Section 599.944	7 pages
Attachment 6, CalHR Information Security Policy Manual	48 pages
Exhibit B – Budget Detail and Payment Provisions	2 pages
Exhibit B-1 – Fee Schedule	1 page
Exhibit C* - General Terms and Conditions	GIA 610
Exhibit D - Special Terms and Conditions	2 pages

Items shown with an Asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.

These documents can be viewed at www.ols.dgs.ca.gov/Standard+Language

IN WITNESS WHEREOF, this Agreement has been executed by the parties hereto.

CONTRACTOR

CONTRACTOR'S NAME *(if other than an individual, state whether a corporation, partnership, etc.)*
Department of Human Resources

BY *(Authorized Signature)* | DATE SIGNED*(Do not type)*

PRINTED NAME AND TITLE OF PERSON SIGNING
Mark T. Rodriguez, Chief, Administrative Services Division

ADDRESS
1515 S Street, North Building, Suite 500
Sacramento, CA 95811

STATE OF CALIFORNIA

AGENCY NAME

BY *(Authorized Signature)* | DATE SIGNED*(Do not type)*

PRINTED NAME AND TITLE OF PERSON SIGNING

ADDRESS

California Department of General Services Use Only

☐ Exempt per:

EXHIBIT A
SCOPE OF WORK

The California Department of Human Resources (CalHR) agrees to provide services to the District Agricultural Association (DAA) <Fair Name> for the processing of payroll deduction data for <Fair Name> employees mandatory participation in the Part-time, Seasonal, and Temporary (PST) Retirement Program, the Alternate Retirement Program (ARP), and voluntary participation in the Savings Plus 401(k) and 457 Plans.

PST Background

In response to the Federal Omnibus Budget Reconciliation Act of 1990, the State established PST as a mandatory retirement program for State employees hired after August 1, 1991 who are not covered by Social Security and are presently excluded from CalPERS because of time base or length of appointment as defined in the Savings Plus 457 Deferred Compensation Plan Document. CaIHR is the administrator of PST as described in Government Code Chapter 8.5, Section 19999.2.

ARP Background

Senate Bill 1105, chaptered August 11, 2004, established the ARP for new state miscellaneous and industrial employees hired between August 11, 2004 and June 30, 2013. The bill created Chapter 8.6 (commencing with Section 19999.3) to Part 2.6 of Division 5 of title 2 of, the Government Code. Government Code Section 19999.3 authorized the creation of a retirement savings program in lieu of retirement service credit and contributions under CaIPERS.

An ARP participant is a state employee who first qualified for membership in the California Public Employees Retirement System (CaIPERS) between August 11, 2004 and June 30, 2013, pursuant to Government Code Section 20281.5. As described in Government Code Section 19999.3(a), the ARP participant does not make contributions into the CaIPERS defined benefit retirement program for the first 24 months of employment following the date he or she qualifies for and becomes a CaIPERS member. Instead, their retirement contributions are deposited into a 401(a) account as allowed by Government Code Section 19999.5. The 401(a) accounts are managed by CalHR. CaIHR is the administrator of ARP as described in Government Code Section 19999.31.

Government Code Section 20908(a) specifies that eligible ARP participants can elect to receive CaIPERS service credit for the time they worked under ARP but for which they did not accrue credit. The election begins on the first day of the 47th month and ends on the last day of the 49th month after their CaIPERS membership date. Government Code Section 20908(b) states that an eligible ARP participant who elects to receive CaIPERS service credit shall cause his or her ARP funds, the accumulated 401(a) contributions including earnings, to be transferred to CaIPERS.

401(K) Plan & 457 Plan Background

The 401(k) Plan and the 457 Plan are the voluntary retirement plans available to certain employees and elected officials of the State of California. Pursuant to California Government Code Section 19999.5 the State of California Savings Plus 401(k) Thrift Plan was established October 15, 1985, as a defined contribution, profit sharing plan, intended to meet the applicable requirements of Section 401(a) of the Internal Revenue Code of 1986, as amended, and contains a cash or deferred arrangement intended to qualify under Section 401(k) of the Code.

Pursuant to California Government Code Section 19993 of the State of California Savings Plus 457 Deferred Compensation Plan was established May 1, 1974. The 457 Plan is an eligible deferred compensation plan intended to meet the applicable requirements of Section 457(b) of the Internal Revenue Code of 1986, as amended. Participation in 401(k) and the 457 Plans is voluntary. State and California State University employees who qualify for membership in the California Public Employees Retirement System, the Legislators' Retirement System (LRS), or the Judges' Retirement System (JRS) are eligible to contribute to the Main Plan.

Services to be Provided
CaIHR and <Fair Name> agree to perform their respective services regarding PST, ARP, 401(k), and 457 Plans in accordance with the terms and conditions set forth herein and as detailed in the following documents, which are attached hereto and by this reference incorporated herein.

Exhibit A, Attachment 1: Statement of Work

Exhibit A, Attachment 2: Deduction Codes

Exhibit A, Attachment 3: File Requirements

Exhibit A, Attachment 4: Sample Contribution Time Table

Exhibit A, Attachment 5: California Administrative Code, title 2, sections 599.944 Article XVII, 599.945 Article XVII.V, 599.946 Article XVII.VI, 599.947 Article XVII.VII, and PMLs 2012-012, 2011-042.

Exhibit A, Attachment 6: CalHR Information Security Policy Manual, and CalHR confidentiality Statement

Exhibit B, Attachment 1, Fee Schedule

Amendments
This Agreement may be amended by mutual consent of the parties. No amendment or variation of the terms of this Agreement shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or Agreement not incorporated in the Agreement is binding on any of the parties.

Disputes
CalHR and <Fair Name> agree that notwithstanding the existence of a dispute between <Fair Name> and CalHR, they will continue without delay to carry out all their responsibilities under this Agreement.

Entire Agreement
This Agreement contains all representations and the entire understanding between the parties hereto with respect to the subject matter hereof. Any prior correspondence, memoranda or agreements are replaced in total by this Agreement.

EXHIBIT A, ATTACHMENT 1
STATEMENT OF WORK

PAYROLL DEDUCTION FILES

<Fair Name> agrees to submit accurate payroll deduction data in accordance with the terms and timing set forth by the California Department of Human Resources (CalHR) as stated herein. If no payroll data is available because there were no employee deductions to report during any given processing period, <Fair Name> must notify CalHR accordingly so that a zero dollar file may be approved. CalHR conducts quarterly audits of deduction data. CalHR will impose a fee per file per quarter for which no data or notification was received. Review the fee schedule in Exhibit B for details. The fee will be assessed on a quarterly basis as a result of the audit, as outlined in the CalHR Fee Schedule.

California Administrative Code, title 2, sections 599.944 Article XVII, 599.946 Article XVII.VI, and Policy Memo 2011-42, require that 401(k) and 457 plans withholdings post by the first business day following the prior pay period. For ARP and PST plans, withholdings must post as soon as practicable, but no later than 15 business days after the paycheck was issued that reflects the deduction. Loan repayments must be submitted with the month-end payroll. A loan repayment must begin with the pay period it's reported as a new deduction on the 650 Report and continue until a stop notification is received on a future 650 Report.

MAIN PLAN (401(K) AND 457 PLANS)

Main Plan deductions include pre-tax, designated Roth, and deductions for up to two loan repayments per plan for a maximum of four loans. Under no circumstance is the <Fair Name> or any of its subsidiaries authorized to impose an independent processing fee to its employees for deductions related to any of the Savings Plus plans.

<Fair Name> is responsible for reviewing deduction files for accuracy prior to submitting to CalHR.

650 REPORT

The 650 report applies to 401(k) and 457 main plan deductions such as pre-tax, designated Roth, and loan repayment deductions.

<Fair Name> employees who are eligible for membership in the California Public Employees' Retirement System (CalPERS) are entitled to contribute to the Main Plan as part of the State employment benefit package. Their participation is not subject to <Fair Name> approval nor are they required to submit any additional forms beyond those provided by Savings Plus.

CalHR reports to <Fair Name> of new employees deductions, deduction changes, and deduction stops, made by an employee by posting the 650 report on the CalHR Extranet no later than the 4th business day of each month. In most cases <Fair Name>'s designated representative will receive an email notification when the 650 report includes requests from <Fair Name> employees.

<Fair Name> is responsible for inputting the employee's request in its payroll system so that the deduction is taken from the employees payroll within the same month and reported to CalHR on the next payroll deduction file.

Failure to process the 650 report may result in the participant's account becoming underfunded. California Administrative Code , title 2, sections 599.944 Article XVII, 599.946 Article XVII.VI, and PMLs 2012-012, 2011-042 requires the entity responsible for the error to pay:

All lost earnings that would have been deposited in the account if the error had not occurred[1].
Five hundred dollars ($500.00), per underfunded account, to cover administrative costs.
Corrective contributions equal to 50% of the deduction amount an employee elected but was unable to make[2].

The entity responsible for the error may not deduct from or offset the funding against any employee's compensation. CalHR will determine the amount of lost earnings required to make the account whole.

CalHR provides the following sites to facilitate timely payroll deduction reporting:

SUBMIT PAYROLL DEDUCTION FILES ELECTRONICALLY

FTP Site: https://ftp.dpa.ca.gov

<Fair Name> may use the FTP site as a secure way to submit electronic payroll deduction files to CalHR. Electronic files must follow CalHR file format requirements. <Fair Name> is responsible for logging into the CalHR extranet following submission of an electronic file and ensuring that the data loaded correctly and reflects the correct file total. CalHR will reject any files in which the deductions within the file do not reconcile to the total amount shown in the file footer or in which the file total does not reconcile to the ACH total. In cases in which the file does not reconcile, the file will be considered delinquent, and will be subject to delinquency fees as outlined in California Administrative Code, title 2, sections 599.944 Article XVII, 599.945 Article XVII.V, 599.946 Article XVII.VI, 599.947 Article XVII.VII.

RETRIEVE 650 REPORT AND UPDATE OR CORRECT PAYROLL DEDUCTIONS

CalHR Extranet https://portal.dpa.ca.gov/eapps/fairscontribution/

<Fair Name> will use the CalHR extranet site to retrieve its monthly 650 Report and follow through to ensure the participants voluntary deduction requests are processed and reported to CalHR in compliance with the CalHR Contribution Schedule so that the participant's deductions post by the first business day following the prior pay period as outlined in CalHR PML 2011-42. Additionally, <Fair Name> will log in to the CalHR extranet following submission of an electronic file to ensure that data loaded correctly and reflects the correct file total. CalHR will reject any files that do not reconcile to the ACH total. In cases in which the files do not reconcile, the file will be considered delinquent, subject to delinquency fees as outlined in California Administrative Code, title 2, sections 599.944 Article XVII, 599.945 Article XVII.V, 599.946 Article XVII.VI, 599.947 Article XVII.VII.

<Fair Name> may also use the CalHR extranet site to manually enter payroll deduction data and make changes or corrections to deduction data previously entered or uploaded electronically, provided <Fair Name> does so before the end of the processing period as reflected in the contribution table provided annually by CalHR. Refer to Attachment 4.

An accurate and timely file is defined as:
A payroll deduction file or payroll deduction data received either electronically or entered manually on the CalHR Extranet before the end date and time for each processing period as reflected in the contribution time table. Refer to Attachment 4.

1 Lost earnings are not imposed on missed main plan deductions, only ARP, PST, and Lump Sum deductions.

[2] *If the error occurs in the first 3-months of the plan year and the employee was able to make deferrals during the last 9-months of the year (April to December) up to the applicable maximum limit, the 50% corrective contribution is not required.*

A payroll deduction file or payroll deduction data received either electronically or entered manually on the CalHR Extranet in good order within the processing period so that the name and format meet CalHR file requirements and the total amount reported reconciles to the corresponding fund transfer.
A payroll deduction file or payroll deduction data accompanied by a corresponding fund transfer in accordance with the fund transfer protocols set forth in this document and reflected in the annual contribution time table provided annually by CalHR and which reconciles to the exact amount of the payroll deduction file provided by <Fair Name>.

Files that are not received timely, accurately, or that do not accompany a corresponding and reconcilable fund transfer will be rejected and deemed delinquent. Delinquent files are subject to late fees as outlined in this document and within the California Administrative Code, title 2, sections 599.944 Article XVII, 599.945 Article XVII.V, 599.946 Article XVII.VI, 599.947 Article XVII.VII, and PMLs 2012-012, 2011-042.

INFORMATION SECURITY & CONFIDENTIALITY
<Fair Name> will adhere to the CalHR Information Security Policy and Confidentiality Statement as set forth therein when accessing, transmitting, or retrieving secure and confidential data through CalHR web based applications.

DEDUCTION TIMETABLES
<Fair Name> will submit payroll deduction data in accordance with the deduction timetable provided annually by CalHR. CalHR creates the deduction timeline as an all-encompassing system in consideration of the State Controller's Office (SCO) pay cycles and other external dependencies and as such the timing of its production is dependent upon the availability of SCO payroll dates.

FUND TRANSFERS

<Fair Name> agrees to transfer funds electronically as soon as administratively feasible following each payroll deduction file, but not later than the date reflected in the deduction time table provided annually by CalHR and as outlined in California Administrative Code, title 2, sections 599.944 Article XVII, 599.946 Article XVII.VI, and Policy Memo 2011-42. <Fair Name> may submit payroll deduction funds via wire transfer or ACH according to its preference.

JP Morgan Chase Bank
Account # 900-9000-127
ABA# 021000021
Name: PTFS Operations
FFC: P35664 State of Cal *(No space between P and 3)***.**

<Fair Name> will notify CalHR of the impending fund transfer by sending an email to: anthony.v.sottile@jpmorgan.com, catherine.hoang@calhr.ca.gov, and sarah.ketchum@calhr.ca.gov.

The email will include the date of the fund transfer and the following detailed breakdown:
401(k) Deduction total = $xxxx.xx
401(k) Loan total = $xxxx.xx
457 Deduction total = $xxxx.xx
457 Loan total = $xxxx.xx
ARP Deduction total = $xxxx.xx
PST Deduction total = $xxxx.xx

CALHR ADMINISTRATIVE FEES

ARP and PST fees are as follows (there are no fees for Main Plan deductions):
ARP **per deduction (positive and negative)** fee: $4.80
PST **per deduction (positive and negative)** fee: $2.45
401(k) / 457 deduction fee $0.00

<Fair Name> will submit payment and a breakdown of all ARP and PST Administrative Fees to CalHR within 30 days of the conclusion of each processing period (See CalHR Fee Schedule). <Fair Name> may transmit Administrative Fees either electronically or through paper check as follows:

Mail paper checks to:
Department of Human Resources
1515 “S” Street, Suite 400N
Attn: Cathy Hoang
Sacramento, CA 95811

Electronic fund transfers:
Bank of America
Sacramento Main #1489
555 Capital Mall, Suite 765
Sacramento, CA 95814
For credit to the State of California
Account # 01482-80005
ABA# 0260-0959-3
For further credit to Dept. of Human Resources
Reference: Cathy Hoang (916) 324-9422

Calculating Administrative Fees:

Step 1: Determine number of deductions in ARP (positive and negative deductions) reported during the corresponding processing period and multiply by the ARP per deduction fee ($4.80).

Step 2: Determine number of deductions in PST (positive and negative deductions) reported during the corresponding processing period and multiply by the PST per deduction fee ($2.45).

Timely receipt of administrative fees does not impact CalHR's responsibility to approve and process the payroll deduction file. However, administrative fees should be received by CalHR no more than 30 calendar days after the close of each processing period.

DELINQUENT FILE FEE
IRS requires that participant accounts be made whole if the participant is disadvantaged due to late deduction posting. Late deduction posting imposes an undue hardship on Savings Plus and negatively affects other account services. As such, CalHR will assess a $500.00 administrative fee for each account that is posted late. To avoid the delinquent file fee, CalHR must receive a valid file **and** fund transfer by the due dates reflected in the Fairs Contribution Schedule.

CALHR INFORMATION TECHNOLOGY (IT)
The IT Division is a subsidiary of CalHR and is only available for technical support upon request from authorized CalHR personnel. Under no circumstances should <Fair Name>, its staff, or any subsidiaries therein contact the CalHR IT Division or request technical support directly from CalHR IT. CalHR IT support is subject to approval by Savings Plus at the discretion of authorized personnel therein. Files that require IT intervention may be subject to a fee per infraction as outlined in the CalHR Fee Schedule.

PST TO CalPERS AT 1000 HOUR MARK

<Fair Name> is responsible for submitting PST deductions to CalHR as soon as practicable, but no later than 15 business days after the paycheck was issued that reflects the deduction.

<Fair Name> is also responsible for tracking the number of hours worked by its PST employees. PST employees who work 1,000 or more hours in a fiscal year (July 1 through June 30) are entitled to permanent employment status. is responsible for stopping the PST deductions and coordinating the employee's new retirement deduction directly with CalPERS.

PST deductions that are sent to CalHR in error, may be reversed by <Fair Name> if the correction is made within 90 days of the last PST deduction. Reversal of deduction errors older than 90 days require CalHR approval. CalHR will approve the reversal pending confirmation that the employee has a sufficient balance in the PST account.

ARP DEDUCTIONS

<Fair Name> is responsible for submitting ARP deductions to CalHR as soon as practicable, but no later than 15 business days after the paycheck was issued that reflects the deduction.

The employee's ARP account is considered underfunded if the PST employee reached their 1,000 hour mark between August 11, 2004 and June 30, 2013 but <Fair Name> failed to properly coordinate the deduction change from PST to ARP. This may be the case even if the employee is beyond the ARP decision period.

ARP deductions that are sent to CalHR in error, may be reversed by <Fair Name> if the correction is made within 90 days of the last ARP deduction. Reversal of deduction errors older than 90 days require CalHR approval. CalHR will approve the reversal pending confirmation that the employee has sufficient balance in the ARP account.

LEGAL AUTHORITY

Unless otherwise stated, CalHR's authority to enforce the requirements of this agreement is based on California Administrative Code, title 2, sections 599.944 Article XVII, 599.945 Article XVII.V, 599.946 Article XVII.VI, 599.947 Article XVII.VII

EXHIBIT A – ATTACHMENT 2
DEDUCTION CODES

401(K) Deduction Codes

Type	Deduction Code	Plan Code
Pre-Tax Deduction	029	401
Loan 1 Repayment	075	401
Loan 2 Repayment	075	402
Roth Deduction	075	010

457 Deduction Codes

Type	**Deduction Code**	**Plan Code**
Pre-Tax Deduction	029	457
Loan 1 Repayment	075	457
Loan 2 Repayment	075	458
Roth Deduction	075	011

PST Deduction Code

Type	**Deduction Code**	**Plan Code**
Pre-Tax Deduction	029	999

ARP Deduction Code

Type	**Deduction Code**	**Plan Code**
Pre-Tax Deduction	029	414

EXHIBIT A – ATTACHMENT 3
FILE REQUIREMENTS

Each section of each electronic file will be pipe delimited as follows:

Header Record (first line in file)

Field #	Description	Length	Format	Comment	Required
1	Pay Period Month	2	MM	Month of pay period	R
2	Pay Period Year	4	YYYY	Year of pay period	R
3	Pay Period	1	#	1 – first half 2 – second half	R
4	File Creation Date	8	YYYYMMDD		R
5	Fair Code	4	X(4)		R

Detail Record

Field #	Description	Length	Format	Comment	Required
1	SSN	9	#(9)	No dashes or hyphens	R
2	Last Name	50	X(50)		R
3	First Name	50	X(50)		R
4	Middle Initial	1	X		R
5	Address	255	X(255)	Street Address Ex: 100 Home Street, Apt 345	R
6	City	25	X(25)		R
7	State	2	X(2)		R
8	ZIP Code	5	#(5)		R
9	Birth date	8	YYYYMMDD		R
10	Rehired Annuitant Code	1	X	Optional field, can be blank: R – Rehired Annuitant	NR
11	Annualized Base Salary	10	#(7).#(2)	Annual Salary Rate – **for 401(k) and 457 only**	R
12	Tran Code	3	X(3)	Employment Status codes • A01 – Active EE • S01 – Terminated/Separated EE • S95 – EE is deceased • M01 – Military Leave • E01 –Medical Leave	R
13	Status Effective Date	8	YYYYMMDD	Employment status effective date is required if there is a change in employment status (Field 12).	NR

Field #	Description	Length	Format	Comment	Required
14	Deduction Code	3	#(3)	029 – Contribution 075 – After-Tax Deduction (Loans & Roth)	R
15	Plan Code	3	#(3)	Valid Values: • 401 – 401k Plan Contribution / Loan 1 • 402 – 401k Plan Contribution / Loan 2 • 457 – 457 Plan Contribution / Loan 1 • 458 – 457 Plan Contribution / Loan 2 • 010 – Roth 401k • 011 – Roth 457 • 414 – ARP Contribution • 999 – PST Contribution	R
16	Deduction Amount	11	(-)#(7).#(2)	• Contribution Amount (Examples for a $50.75 deduction) • Example 1 = “ 50.75” • Example 2 = “ -50.75” (Negative Amount, floating negative sign)	R

Trailer Record (last line in file)

Field #	Description	Length	Format	Comment	Required
1	Total Record Count	6	#(6)		R
2	Total Deduction Count	6	#(6)		R
3	Total Deduction Amount	12	(-)#(8).#(2)		R

Examples of Deductions and indicative data for all plans (PST, ARP, 401(k) & 457)

Deductions

«DAA»_FairContribution_201211_1.txt

```
11|2012|1|20121110|«DAA»
111223333|Brown|Pat|R|7725 Rocky Road, Apt.B|Elk Grove|CA|95634|19800502|||A01||029|414|25.00
222446666|Moore|Joe||2323 Front St, Ste.345|Sacramento|CA|95828|19600707|||S01|20121105|||0.00
999553232|Smith|John|L|1212 16th St|Sacramento|CA|95820|19751015|R|55000|A01||029|457|50.75
999553232|Smith|John|L|1212 16th St|Sacramento|CA|95820|19751015|R|55000|A01||029|401|100.00
4|3|175.75
```

John Smith has multiple deductions (457 and 401k)
There should be a record for each deduction
His records have an “R” in the field after his DOB to indicate he’s a rehired annuitant
Annualized Base Salary field is required for 401k or 457 deduction records

Employee Information Change

«DAA»_FairContribution_201211_1.txt
11|2012|1|20121110|«DAA» 111223333|Brown|Pat|R|7725 Rocky Rd, Apt.B22|Elk Grove|CA|95634|19800502|||A01||029|414|25.00 222446666|Moore|Joe||2323 Front St, Ste.345|Sacramento|CA|95828|19600707|||S01|20121105|||0.00 999553232|Smith|John|L|1212 16th St|Sacramento|CA|95820|19751015|R|55000|A01||029|457|50.75 999553232|Smith|John|L|1212 16th St|Sacramento|CA|95820|19751015|R|55000|A01||029|401|100.00 4|3|175.75

Joe Moore has separated
Tran Code (S01) indicates employee is separated
Status Effective Date (20121105) indicates effective date of the employee's separation status

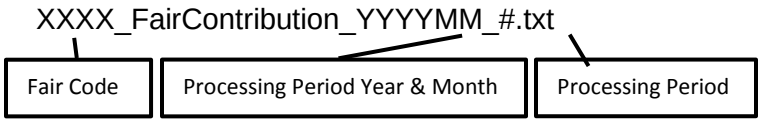
Payroll Adjustment/Reversal

«DAA»_FairContribution_201211_1.txt
11|2012|1|20121110|«DAA» 123553232|Smith|Jane|L|1212 16th St, Ste.345|Sacramento|CA|95820|19751015|R||A01||029|999|500.00 1|1|500.00

Employer overpays a PST employee
Pay was calculated for 70 hours for a PST deduction of $500 and employee only worked 50 hours
Employer submits a payroll adjustment/reversal of -$150 on the next file along with normal deduction

«DAA»_FairContribution_201211_2.txt <- Next pay period file
11|2012|2|20121123|«DAA» 123553232|Smith|Jane|L|1212 16th St|Sacramento|CA|95820|19751015|R||A01||029|999|300.00 123553232|Smith|Jane|L|1212 16th St|Sacramento|CA|95820|19751015|R||A01||029|999|-150.00 2|2|150.00

Naming Convention
The file name is a coded formula that allows CalHR systems to automatically recognize and process the file as soon as it's received. For that reason, the file name must be exact. The file name will contain the fair code, pay period year and month, and the processing period as follows:



File Totals
Files contain total deduction which may be used to cross check what was manually keyed. This will help identify any typos or human errors before the processing period closes.

The file total is the last row of the file and it only contains three fields. For example:

183|183|11842.15

Total Record count and total record amount.

Checklist

Task Name	Task Description
File name is correct:	XXXX_FairContribution_YYYYMM_#.txt Fair Code · Processing Period Year & Month · Processing Period
File Header is correct:	02|2014|1|20140206|50XX Month · Processing Period Year · Processing Period · File Creation · Fair Code
Format is Correct	Pipe delimited, with at least 15 pipes across each row. State should always say "CA" not cali, or Cali, or Ca. Also the city and state should be separated by a pipe delimitation. **11|2012|2|20121123|«DAA»**
Deduction total is correct:	After you submit your FTP file. Review the last line in your file which is the trailer record. It contains 3 pipe delimited sections as follows: Total number of records, Total number of deductions, and the Total Deduction amount. Make sure the total deduction amount is identical to the penny when compared to total deductions in the Extranet site.

EXHIBIT A, ATTACHMENT 4
SAMPLE CONTRIBUTION TIME TABLE

2	3	4	5	6
Key or upload data.	**Provide funding via ACH or wire to JP Morgan**	**CalHR Accting delivers claim schedules to SCO.**	**CalHR Accting emails Investment Summary to Aon Hewitt. Aon Hewitt reviews deduction details.**	**Aon Hewitt posts transactions.**
Within date range (by no later than 11:59 pm on last day)	**By 4:00 pm on date below**	**By 10:00 am on date below**	**By COB on date below**	**By COB Eastern Time on date below.**
12/17/2014 - 12/27/2014	**12/30/2014**	**12/31/2014**	**12/31/2014**	**1/2/2015**
1/5/2015 - 1/13/2015	**1/14/2015**	**1/15/2015**	**1/15/2015**	**1/16/2015**
1/20/2015 - 1/27/2015	**1/28/2015**	**1/29/2015**	**1/29/2015**	**1/30/2015**
2/2/2015 - 2/11/2015	**2/12/2015**	**2/13/2015**	**2/13/2015**	**2/17/2015**
2/18/2015 - 2/25/2015	**2/26/2015**	**2/27/2015**	**2/27/2015**	**3/2/2015**
3/3/2015 - 3/11/2015	**3/12/2015**	**3/13/2015**	**3/13/2015**	**3/16/2015**
3/17/21013 - 3/26/2015	**3/27/2015**	**3/30/2015**	**3/30/2015**	**4/1/2015**
4/2/2015 - 4/13/2015	**4/14/2015**	**4/15/2015**	**4/15/2015**	**4/18/2015**
4/20/2015 - 4/28/2015	**4/29/2015**	**4/30/2015**	**4/30/2015**	**5/1/2015**
5/4/2015 - 5/13/2015	**5/14/2015**	**5/15/2015**	**5/15/2015**	**5/18/2015**
5/19/2015 - 5/27/2015	**5/28/2015**	**5/29/2015**	**5/29/2015**	**6/1/2015**
6/2/2015 - 6/11/2015	**6/12/2015**	**6/15/2015**	**6/15/2015**	**6/16/2015**
6/17/2015 - 6/26/2015	**6/29/2015**	**6/30/2015**	**6/30/2015**	**7/1/2015**
7/2/2015 - 7/13/2015	**7/14/2015**	**7/15/2015**	**7/15/2015**	**7/16/2015**

2	3	4	5	6
Key or upload data.	**Provide funding via ACH or wire to JP Morgan**	**CalHR Accting delivers claim schedules to SCO.**	**CalHR Accting emails Investment Summary to Aon Hewitt. Aon Hewitt reviews deduction details.**	**Aon Hewitt posts transactions.**
Within date range (by no later than 11:59 pm on last day)	**By 4:00 pm on date below**	**By 10:00 am on date below**	**By COB on date below**	**By COB Eastern Time on date below.**
7/17/2015 - 7/28/2015	**7/29/2015**	**7/30/2015**	**7/30/2015**	**7/31/2015**
8/3/2015 - 8/12/2015	**8/13/2015**	**8/14/2015**	**8/14/2015**	**8/17/2015**
8/18/2015 - 8/27/2015	**8/28/2015**	**8/31/2015**	**8/31/2015**	**9/1/2015**
9/2/2015 - 9/11/2015	**9/14/2015**	**9/15/2015**	**9/15/2015**	**9/16/2015**
9/17/2015 - 9/28/2015	**9/29/2015**	**9/30/2015**	**9/30/2015**	**10/1/2015**
10/2/2015 - 10/13/2015	**10/14/2015**	**10/15/2015**	**10/15/2015**	**10/16/2015**
10/19/2015 - 10/28/2015	**10/29/2015**	**10/30/2015**	**10/30/2015**	**11/2/2015**
11/3/2015 - 11/10/2015	**11/12/2015**	**11/13/2015**	**11/13/2015**	**11/16/2015**
11/17/2015 - 11/25/2015	**11/30/2015**	**12/1/2015**	**12/1/2015**	**12/2/2015**
12/3/2015 - 12/11/2015	**12/14/2015**	**12/15/2015**	**12/15/2015**	**12/16/2015**
12/17/2015 - 12/29/2015	**12/30/2015**	**12/31/2015**	**12/31/2015**	**1/4/2016**

EXHIBIT A – ATTACHMENT 5
CALIFORNIA ADMINISTRATIVE CODE TITLE 2, SECTION 599.944

2 CCR § 599.944

Cal. Admin. Code tit. 2, § 599.944

Barclays Official California Code of Regulations Currentness
Title 2. Administration
Division 1. Administrative Personnel
Chapter 3. Department of Personnel Administration
Subchapter 1. General Civil Service Rules
Article 27. 457 Deferred Compensation Plan
§ 599.944. Corrective Contributions and Lost Earnings.

a) If an employee directed contribution transaction is not processed appropriately causing the employee's 457 Deferred Compensation Plan account to be underfunded, it is the responsibility of the entity that made the error to make the account whole. This includes all corrective contributions and lost earnings that would have been deposited in the account if the error had not occurred. The entity responsible will also be required to pay five hundred dollars ($500), per underfunded account, to cover administrative costs.
b) If contributions made by, or for, an employee under the 457 Deferred Compensation Plan are not deposited in the employee's Plan account by the date required by federal law, state law, or regulations governing the Plan, the entity responsible for the error must pay all lost earnings that would have been deposited in the account if the error had not occurred. The entity responsible will also be required to pay five hundred dollars ($500), per underfunded account, to cover administrative costs.
c) Corrective contributions and any lost earnings as addressed in (a) and (b) above, will be funded by the entity responsible for the error and may not be deducted from or offset against any employee's compensation.
d) The California Department of Human Resources will determine the amount of lost earnings required to make the account whole.
e) The California Department of Human Resources will receive reimbursement for the corrective contributions, any lost earnings, and administrative costs through the State Controller's Office in accordance with Government Code Section 11255. The State Controller's Office and the California Department of Human Resources shall each receive one half of the five hundred dollar administrative fee paid by the responsible entity. If the responsible entity is not a state agency subject to Government Code Section 11255, the California Department of Human Resources will obtain reimbursement directly from the entity, and shall retain the full amount of any administrative fee collected from the entity.

Note: Authority cited: Section 19815.4, Government Code; and Article XVI, Section 17, California Constitution. Reference: Section 19993, Government Code.

HISTORY
1. New section filed 10-22-2012; operative 11-21-2012 (Register 2012, No. 43).

2 CCR § 599.944, 2 CA ADC § 599.944

This database is current through 10/26/12 Register 2012, No. 43

END OF DOCUMENT

2 CA ADC § 599.945.4
§ 599.945.4. Corrective Contributions and Lost Earnings.

Cal. Admin. Code tit. 2, § 599.945.4
Barclays Official California Code of Regulations Currentness
Title 2. Administration
Division 1. Administrative Personnel
Chapter 3. Department of Personnel Administration
Subchapter 1. General Civil Service Rules
Article 27.5. Part-Time, Seasonal and Temporary (Pst) Employee Retirement Program

§ 599.945.4. Corrective Contributions and Lost Earnings.

a) If an employee is not properly placed in the Part-time, Seasonal and Temporary (PST) Employee Retirement Program when he or she becomes eligible or if a transaction is processed inappropriately causing the employee's PST account to be underfunded, it is the responsibility of the entity that made the error to make the account whole. This includes all corrective contributions and lost earnings that would have been deposited in the account if the error had not occurred. The entity responsible will also be required to pay five hundred dollars ($500) per underfunded account to cover administrative costs.
b) Corrective contributions and any lost earnings will be funded by the entity responsible for the error and may not be deducted from or offset against any employee's compensation.
c) The entity processing the correction will determine the amount of corrective contributions. The California Department of Human Resources will determine the amount of the lost earnings required to make the account whole.
d) The California Department of Human Resources will receive reimbursement for the corrective contributions, any lost earnings, and administrative costs through the State Controller's Office in accordance with Government Code 11255. The State Controller's Office and the California Department of Human Resources shall each receive one half of the five hundred dollar administrative fee paid by the responsible entity. If the responsible entity is not a state agency subject to Government Code Section 11255, the California Department of Human Resources will obtain reimbursement directly from the entity, and shall retain the full amount of any administrative fee collected from the entity.

Note: Authority cited: Section 19815.4, Government Code; and Article XVI, Section 17, California Constitution. Reference: Section 19999.21, Government Code.

HISTORY

1. New section filed 11-9-2012; operative 11-9-2012 pursuant to Government Code section 11343.4 (Register 2012, No. 45).

2 CCR § 599.945.4, 2 CA ADC § 599.945.4
This database is current through 1/4/13 Register 2013, No. 1
END OF DOCUMENT

2 CCR § 599.946

Cal. Admin. Code tit. 2, § 599.946

Barclays Official California Code of Regulations Currentness
Title 2. Administration
Division 1. Administrative Personnel
Chapter 3. Department of Personnel Administration
Subchapter 1. General Civil Service Rules
Article 27.6. 401(K) Retirement Savings Plan
§ 599.946. Corrective Contributions and Lost Earnings.

a) If an employee directed contribution transaction is not processed appropriately causing the employee's 401(k) Retirement Savings Plan account to be underfunded, it is the responsibility of the entity that made the error to make the account whole. This includes all corrective contributions and lost earnings that would have been deposited in the account if the error had not occurred. The entity responsible will also be required to pay five hundred dollars ($500), per underfunded account, to cover administrative costs.
b) If contributions made by, or for, an employee under the 401(k) Retirement Savings Plan are not deposited in the employee's Plan account by the date required by federal law, state law, or regulations governing the Plan, the entity responsible for the error must pay all lost earnings that would have been deposited in the account if the error had not occurred. The entity responsible will also be required to pay five hundred dollars ($500), per underfunded account, to cover administrative costs.
c) Corrective contributions and any lost earnings as addressed in (a) and (b) above, will be funded by the entity responsible for the error and may not be deducted from or offset against any employee's compensation.
d) The California Department of Human Resources will determine the amount of lost earnings required to make the account whole.
e) The California Department of Human Resources will receive reimbursement for the corrective contributions, any lost earnings, and administrative costs through the State Controller's Office in accordance with Government Code 11255. The State Controller's Office and the California Department of Human Resources shall each receive one half of the five hundred dollar administrative fee paid by the responsible entity. If the responsible entity is not a state agency subject to Government Code Section 11255, the California Department of Human Resources will obtain reimbursement directly from the entity, and shall retain the full amount of any administrative fee collected from the entity.

Note: Authority cited: Section 19815.4, Government Code; and Article XVI, Section 17, California Constitution. Reference: Section 19999.5, Government Code.

HISTORY

1. New article 27.6 (section 599.946) and section filed 10-22-2012; operative 11-21-2012 (Register 2012, No. 43).

2 CCR § 599.946, 2 CA ADC § 599.946

This database is current through 10/26/12 Register 2012, No. 43

2 CCR § 599.947

Cal. Admin. Code tit. 2, § 599.947

Barclays Official California Code of Regulations Currentness
Title 2. Administration
Division 1. Administrative Personnel
Chapter 3. Department of Personnel Administration
Subchapter 1. General Civil Service Rules
Article 27.7. Alternate Retirement Program (ARP)
§ 599.947. Corrective Contributions and Lost Earnings.

a) If an employee is not properly placed in the Alternate Retirement Program when he or she becomes eligible, or within 90 days thereof, the employer shall pay for any corrective contributions and lost earnings necessary to make the account whole, as well as administrative costs of five hundred dollars ($500) per underfunded account.
b) If a transaction is processed inappropriately causing the employee's Alternate Retirement Program account to be underfunded, it is the responsibility of the entity that made the error to make the account whole. This includes all corrective contributions and lost earnings that would have been deposited in the account if the error had not occurred. The entity responsible will also be required to pay five hundred dollars ($500), per underfunded account, to cover administrative costs.
c) Corrective contributions and any lost earnings as addressed in (a) and (b) above, will be funded by the entity responsible for the error and may not be deducted from or offset against any employee's compensation.
d) The entity processing the correction will determine the amount of corrective contributions. The California Department of Human Resources will determine the amount of the lost earnings required to make the account whole.
e) The California Department of Human Resources will receive reimbursement for the corrective contributions, any lost earnings, and administrative costs through the State Controller's Office in accordance with Government Code Section 11255. The State Controller's Office and the California Department of Human Resources shall each receive one half of the five hundred dollar administrative fee paid by the responsible entity. If the responsible entity is not a state agency, subject to Government Code Section 11255, the California Department of Human Resources will obtain reimbursement directly from the entity, and shall retain the full amount of any administrative fee collected from the entity.

Note: Authority cited: Section 19815.4, Government Code; and Article XVI, Section 17, California Constitution. Reference: Section 19999.31, Government Code.

HISTORY

1. New article 27.7 (section 599.947) and section filed 10-22-2012; operative 11-21-2012 (Register 2012, No. 43).

2 CCR § 599.947, 2 CA ADC § 599.947
This database is current through 10/26/12 Register 2012, No. 43
END OF DOCUMENT

Department of Personnel Administration
Memorandum

TO: Personnel Management Liaisons (PML)

SUBJECT: Underfunded Savings Plus Accounts	**REFERENCE NUMBER:** 2011-042
DATE ISSUED: 11/14/11	**SUPERSEDES:**

This memorandum should be forwarded to:

Accounting Officers
Budget Officers
Employee Benefit Officers
Personnel Officers
Personnel Transactions Staff
Personnel Transactions Supervisors

FROM: Department of Personnel Administration
Savings Plus

CONTACT: Kim Madson, Staff Personnel Program Analyst
(916) 323-8489
Fax: (916) 327-1885
Email: Kimberly.Madson@calhr.ca.gov

Effective immediately, State agencies and departments will bear the cost of errors that occur in processing their employees' contributions to the Savings Plus 401(k) and 457 plans, Alternate Retirement Program (ARP), and the Part-time, Seasonal, and Temporary Employees Retirement Program (PST), when these errors cause underfunding of the employee's account.

Under state and federal law, these costs must be borne by the entity responsible for the error, and may not be deducted from or offset against the employee's compensation. Costs include corrective contributions and lost earnings that would have been deposited to the employee's account if the error had not occurred.

The following types of accounting errors and delays can cause an employee's account to be underfunded.

- Department fails to process the employee's withholding to 401(k), 457, ARP, or PST within the required time period, or not at all. (For 401(k) and 457 plans, withholdings must post by the first business day following the prior pay period. For ARP and PST plans, withholdings must post as soon as practicable, but no later than 15 business days after the paycheck was issued that reflects the withholding.)
- Department does not enroll an eligible employee in the 401(k), 457, ARP, or PST program as required. In these cases, the error creates an underfunded account in the program the employee should have been enrolled in.
- Department processes an employee withholding amount that is less than what it should be for that employee's 401(k), 457, ARP, or PST account.

- Department processes a payroll adjustment that results in a negative balance in the employees Savings Plus, ARP, or PST account.

Delayed deferrals involving lump sum payments

In many cases, late deferrals involve lump-sum payments of unused leave balances that many retiring employees opt to have deposited into their Savings Plus accounts. Current statutory timelines for processing these deferrals are especially challenging to meet given the increased number of employees choosing this option.

Current law says employees must submit their request to your personnel office no later than 5 days before separating, and for the deferral to be posted to their account by the following deadline, ***whichever occurs first***:

- 45 days after the separation date, or
- by February 1 of the calendar year after the year of separation.

Given these short timelines, we suggest you encourage employees planning to defer their lump- sum payment to submit their request to your personnel office 30 calendar days before

separating to allow you more processing time. We also plan to propose statutory changes next year to extend the deadlines for posting the deferral.

Corrective payments

For state agencies on the central payroll system, the State Controller's Office will transfer corrective contributions and lost earnings from the responsible entities to DPA, in accordance with Government Code Section 11255. If the responsible entity is not a state agency subject to Government Code Section 11255, DPA will obtain reimbursement directly from the entity.

/s/ Michelle Berklacich

Michelle Berklacich
Administrator
Savings Plus Program

Department of Personnel Administration
Memorandum

TO: Personnel Management Liaisons (PML)

SUBJECT: Underfunded Savings Plus Accounts	**REFERENCE NUMBER:** 2012-012
DATE ISSUED: 5/31/12	**SUPERSEDES:**

This memorandum should be forwarded to:

Accounting Officers
Budget Officers
Employee Benefit Officers
Personnel Officers Personnel Transaction
Staff Personnel Transaction Supervisors

FROM: Department of Personnel Administration
Savings Plus

CONTACT: Kim Madson, Staff Personnel Program Analyst
(916) 323-8489
Fax: (916) 327-1885
Email: Kimberly.Madson@calhr.ca.gov

Beginning October 1, 2012, departments will be charged a $500 fee for each employee whose Savings Plus account is underfunded. This fee helps pay administrative costs associated with correcting the accounts. Refer to PML 2011-042 for details on the types of errors and delays that can result in underfunding an employee's Savings Plus account.

We also want to provide the following information to clarify when an Alternate Retirement Program (ARP) account is considered underfunded for part-time, seasonal and temporary (PST) employees who reach the 1000-hours-per-fiscal-year cap and are subject to ARP. Use the ARP Eligibility Worksheet on DPA's website to determine if the employee must participate in ARP.

If the 505 transaction to convert an employee's retirement from PST to ARP is keyed *more than*

90 days after the employee's ARP effective date, the ARP account is considered underfunded. The department is responsible for funding the missed ARP contributions and lost earnings.

Departments need to work with their Accounting Office to clear the accounts receivables (ARs)

established for the missed ARP contributions. If the 505 is keyed within 90 days of the ARP effective date, it's considered normal processing and the employee is responsible for funding the AR.

/s/ Michelle Berklacich

EXHIBIT A, ATTACHMENT 6
INFORMATION SECUIRTY POLICY MANUAL

Table of Contents

INTRODUCTION

Information resources in the California Department of Human Resources ("Department" or "CalHR") are strategic and vital assets belonging to the people of California. The Department, as custodian of these assets, is required to ensure the integrity, availability, accountability, confidentiality, and auditability of these assets.

Protection of these assets from accidental or unauthorized access, disclosure, modification or destruction is guided by the issuance of information security policy and procedures. Information security includes information technology hardware and/or software encompassing its lifecycle from procurement to disposal, authorized users access, conduct, responsibilities and education in the use of the Department's information resources and data, both electronic and paper.

Effective security is a team effort involving the participation and support of every Department employee, student assistant, contractor and volunteer who deal with information and/or information systems. It is the responsibility of every authorized user to know these guidelines, and to conduct their activities accordingly.

PURPOSE

The Information Security Manual, published and maintained by the Information Security Office, is the repository for the Department's approved information security policies.

Information security policies are important because they will:

1. protect users and the Department from illegal or harmful actions
2. increase awareness of information security
3. establish accountability for authorized users
4. ensure privacy for the Departments' resources
5. guide product selection and application development
6. achieve consistency in security application and adherence
7. outline acceptable use of computer equipment

The overall objective of the Information Security Policy Manual is to document the policies and procedures that comprise the Department's Information Security Program. These policies are designed to convey information security responsibilities while allowing program units the flexibility to effectively and efficiently meet their business needs.

SCOPE

This Policy Manual applies to all authorized users, which includes all department employees, contractors, student assistants, and volunteers.

ENFORCEMENT

Violation of the policies contained in this manual and/or abuse of the department's computer resources may result in disciplinary action, up to and including possible termination, and/or civil/criminal liability.

Exceptions to the policies will be considered only when the requested exception is documented using appropriate forms submitted to the Chief Information Officer (CIO) and Information Security Officer (ISO) for approval.

RESPONSIBILITIES
Department/Agency

The Department must develop and maintain policies on information security and risk management and ensure compliance with these policies through enforcement, analysis, annual training and auditing. State Administrative Manual (SAM) Section 5300.3

IT Management (Data/Information Custodian)

The Department CIO must ensure the necessary technical means are in place to preserve the security and integrity of the Department's Information Resources and manage the risks associated with those assets and serve as custodians of information. SAM Section 5320.3

Divisions (Data/Information Owners)

The Division Chief's must ensure authorized users are provided the department's information security policies either electronically or by hard-copy. They must also specify and monitor the integrity and security of information resources and the use of those assets within their areas of responsibility. SAM Section 5320.2

Authorized Users

Authorized Users are department employees, contractors, student assistants and volunteers. Authorized users must use department information resources only for authorized purposes in accordance with their job duties and they must comply with all applicable laws and administrative policies. SAM Section 5320.4
NOTE:

Authorized users may not expect or assert a right of privacy in anything they access, create, store, send, or receive using department computer resources unless protected by attorney/client privilege.

The Department reserves the right to access and review all materials created, stored, sent, or received by the user through any department computer, network, service, or Internet/ Intranet/ Extranet connection.

The Department reserves the right to monitor and log any and all aspects of its computer systems including, but not limited to, Internet sites visited by users, chat, blogs and newsgroups, file downloads, file executions and all communications sent and received by users.

The Department reserves the right to conduct risk analysis checks of the department's networks and resources.

ACCEPTABLE USE

Overview

The Department computers and associated networks are owned by the State of California and provided to employees, student assistants, contractors, and volunteers for official State business only. Inappropriate use exposes the computer network to various risks including viruses that may compromise the network systems and services. Inappropriate use also may create legal issues that expose the department to litigation and unnecessary expense in terms of both money and lost productivity.

Policy

This policy sets forth the general principles that govern the acceptable use of California Department of Human Resources' ("Department" or "CalHR") Information Technology (IT) network and services, personal computers (PC), and electronic mail (e-mail) system, including e-mail systems accessed via Department resources.

General principles covered include use of systems and network, user responsibilities, Department responsibilities, and disclosure.

At no time is the Department's network, services, or resources to be used:

For personal advantage, gain or profit.

For any illegal activity.

To conduct, engage, or solicit any activities that violate any state, federal or local laws, regulations, rules, executive orders, agency or department regulations, policies or directives.

2.1 Acceptable Use of Systems and Network

All computer activities must be conducted in a professional, lawful, and ethical manner.

The computer network is the property of the Department and is to be used for legitimate business purposes.

Communication of Confidential Information – Unless expressly authorized by the Deputy Director, Director, or their designee, authorized users are prohibited from sending, transmitting, or otherwise distributing proprietary, confidential, sensitive, privileged or other state government intellectual property. Confidential information can include internal department reports, policies, procedures, attorney-client communications, doctor-client communications or other internal communications. For example, information related to advice received regarding pending litigation against the employee's agency/department or the Social Security and/or driver's license numbers of members of the public which an employee obtains during the course of their duties as a state employee cannot be disseminated. Unauthorized dissemination of such material may result in severe disciplinary action, as well as substantial civil and criminal penalties under state and federal laws.

To ensure security and avoid malware, computers connected to the Department network must be connected through an approved connection.

2.2 Authorized Users Responsibilities

Adhere to information security policies and procedures.

Conserve bandwidth and storage capacity by not engaging in activities that will monopolize resources to the exclusion of others.

Report any security weaknesses or incidents.

Do not intentionally attempt to view, copy, or modify data, documents, e-mail correspondence, or programs that you are not the owner of or do not have authorized access to.

Do not engage in any activity that is illegal under local, state, federal or international law while using department-owned resources.

2.3 Electronic Mail (e-mail)

The Department's e-mail system and services are state department resources. They are provided as a business communication tool and are a means to achieve the Department's mission, values, vision, goals, and business objectives. E-mail includes messages created, sent, received, or retained and any attachments. All messages distributed via the department's e-mail system are the property of the department. Communications and information exchanges directly relating to the mission, goals, and work tasks of the department and announcements of state laws, procedures, policies, services or activities authorized by the department are examples of appropriate use of the department's e-mail and business communication systems. When using the e-mail or department information system the following rules apply:

E-mails sent formally (distribution list) or informally (reply all) must be sent with care. The sender must determine if each member of the group has a need to know and view the information within the e-mail.

Messages containing confidential information should only be sent to individuals who have a legitimate business need to view the information and must be sent securely if sent outside the Department.

The Department's network may not be used to disseminate, access, or store personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan Horse programs, etc.), or any other unauthorized materials.

Forwarding or sending e-mail containing sensitive, personal, and/or confidential information from the Department's e-mail system to any personal e-mail account maintained on Internet Service Providers (ISP) and/or public/private e-mail systems is prohibited.

Automatically (using the auto forward rule) forwarding business-related e-mail from the Department's e-mail system to any personal e-mail account maintained on ISP and/or public/private e-mail systems is prohibited.

Automatically forwarding e-mail to the Department's e-mail system from any personal e-mail account maintained on ISP and/or public/private e-mail systems is prohibited.

Forwarding or sending e-mail containing offensive, malicious, obscene, threatening, intimidating, disparaging, defamatory and invading another's right to privacy or that might constitute harassment or bullying is prohibited.

Examples: Offensive e-mail meant to intentionally harm someone's reputation or that could contribute to a hostile work environment on the basis of race and sex, disability, religion or any other status protected by law or Department policy is prohibited.

Forwarding or sending e-mail that violates the Discrimination and Harassment Prevention, Workplace Violence Prevention and Incompatible Activities is prohibited.

Forwarding or sending e-mail that could constitute retaliation against another employee for reporting a possible deviation from this policy or for cooperation in an investigation is prohibited. Noncompliance with these rules may subject the violator to possible disciplinary action as well as any action that may be taken pursuant to state and federal law.

2.4 Internet/Intranet

The Internet is a tool provided for the sole purpose of performing state job duties. Authorized users are cautioned that the Internet may include websites or pages that contain offensive, sexually explicit, and/or inappropriate material. The following rules apply regarding the Internet/Intranet:

Authorized users shall not access sites that promote illegal, sexual, or other information that would be inconsistent with this and other departmental policies.

Bypassing the Department's computer network security is strictly prohibited.

Department information intended for the general public to be published, posted, or uploaded to a public website on the Internet is considered official department correspondence and must be approved.

Use of the Internet is provided for business-related uses. Unacceptable use includes, but is not limited to, playing games, engaging in online chat groups, gambling, uploading or downloading non-business related files, accessing non-business related streaming audio and/or video files, etc.

Downloading, copying or sharing unlicensed software protected by copyright law from Internet sources is prohibited.

The Department reserves the right to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace and/or violates this and other departmental policies.

2.5 Incidental Use

Government Code Section 8314 permits incidental personal use of State resources. This means:

Incidental personal use of e-mail, internet access, fax machines, printers, and copiers is restricted to approved authorized users only and does not include family members or others not affiliated with or authorized as a user by the Department.

Incidental use must not cause legal action against, or cause embarrassment to the Department

Incidental use must not interfere with the normal performance of an employee's work duties.

Storage of personal e-mail messages, voice messages, files and documents within the Department's computer resources must be nominal.

Department management will resolve incidental use questions and issues using these guidelines in collaboration with the Chief Information Officer (CIO), Information Security Officer (ISO), Human Resources (HR) Chief and Chief Counsel.

Terms and Definitions

Computer Resources

Any and all systems, equipment, and software owned by the department or state, including, but not limited to the Department's IT network and services, personal computers, laptops, thumb drives, e-mail systems, cell phones, and internet/intranet connections.

Data

Factual information, especially information organized for analysis or used to reason or make decisions.

E-mail

The electronic transmissions of information through a mail protocol ("a set of conventions governing the treatment and formatting of data in an electronic communications system" (Merriam Webster)) such as Simple Mail Transfer Protocol (SMTP) or Internet Message Access Protocol (IMAP). Typical e-mail clients include Microsoft Outlook.

Internet

A worldwide network of computers that contain millions of pages of information.

Intranet

A privately maintained computer network that can be accessed only by authorized persons, especially members or employees of the organization that owns it.

Malware

Includes software such as viruses, worms, and Trojan horses with the intent to cause harm. Malware interferes with normal computer functions or sends personal data about the user to unauthorized parties over the internet.

Confidential Information

Proprietary, sensitive, privileged material or other state government intellectual property. This also includes information maintained by state agencies that may be exempt from disclosure under applicable state or federal laws such as the California Public Records Act (Government Code Sections 6250-6265).

Proprietary Information

Information used, made, or marketed by one having the exclusive legal right or a protectable legal interest.

Unauthorized Dissemination

The intentional or unintentional revealing of restricted information to people, both inside and outside the Department, who do not have a need to know that information.

SENSITIVE AND CONFIDENTIAL INFORMATION

1.0 Overview

Sensitive information can be stored, displayed and transported on many kinds of media.

Many of these media are casually removable and portable, including paper, microform, CD, DVD, external hard drives, and flash drives.

Other media are not as casually removable, including computer internal hard drives.

Modes of transportation include e-mail, US mail or by messenger services.

All media is subject to theft by someone who:

Breaks or bypasses the visual security of the work or home office, including seeing computer screens, forms, and other documents containing confidential information;

Breaks or bypasses the physical security of the work or home office; or

Breaks or bypasses the electronic security of department computers and networks.

Intercepts e-mail communication or receives e-mail inadvertently.

Intercepts or receives U.S. mail or messages intentionally or unintentionally

2.0 Purpose

The Information Sensitivity and Confidential Policy is intended to help authorized users determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the Department.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means.

All authorized users should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect the Department's Confidential Information.

3.0 Scope

Department information is categorized into two main classifications:

CalHR Public

CalHR Confidential

CalHR Public Information is information maintained by state departments (agencies) that is not exempt from disclosure under the provisions of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.

CalHR Confidential Information contains all other information including proprietary, sensitive, privileged or other state government intellectual property. Information in this category is positioned on a continuum of sensitivity and confidentiality. Some information in this category is more sensitive than other types of information, and should be protected in a more secure manner and in some cases, never distributed. Confidential information can include internal department reports, policies, procedures attorney-client communications, doctor-client communications and other internal policy decision communications. It can also include information related to advice received regarding pending litigation against the department, Social Security and driver's license numbers, bank account information, and medical and psychological information an employee obtains during the course of their duties.

CalHR Confidential Information also encompasses information provided to CalHR from a third party. This is confidential information belonging or pertaining to another entity which has been entrusted to CalHR by that entity under non-disclosure agreements and other contracts. Examples of this type of information include Scanned Answer sheets from other state agencies/departments.

CalHR staff is encouraged to use common sense judgment in securing CalHR's Confidential Information. If you are uncertain of the sensitivity of a particular piece of information, you should contact your immediate supervisor.

4.0 Policy

Deputy Directors, Division Chiefs, Program Managers, Office Managers, and Supervisors are responsible for ensuring that authorized users are informed and abide by this policy.

Authorized users, including all department employees, contractors, and student assistants are required to take steps to secure sensitive information and prevent unauthorized access.

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as CalHR information in this section may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the CalHR Confidential Information involved.

4.1 Minimal Sensitivity: This category applies to general Department information and some personnel and technical information.

4.1.1 Designation of Material in Hardcopy or Electronic Form.

Marking material is at the discretion of the owner or custodian of the information. If marking is desired, the words "CalHR Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "CalHR Proprietary" or similar labels at the discretion of your individual unit or division. You may want to use the additional label "3rd Party Confidential" if appropriate. Even if no marking is present, CalHR information is presumed to be "CalHR Confidential" unless expressly determined to be CalHR Public Information by CalHR staff with authority to do so.

Access: CalHR employees, contractors, people with a business need to know

Distribution within CalHR: Standard interoffice mail, approved e-mail and electronic file transmission methods.

Distribution outside of CalHR internal mail: U.S. mail and other public or private carries, approved e-mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it is sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines (i.e. computers, fax machines, printers, etc.) should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on CalHR premises. Electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution.

4.2 Moderately Sensitive: This category applies to Department, financial, technical, and most personnel information.

4.2.1 Designation of Material in Hardcopy or Electronic Form.

Marking information as sensitive and confidential is discretionary. Material may be marked at the discretion of your individual unit or division. As the sensitivity level of the information increases, you may, in addition to or instead of marking the information simply "CalHR Confidential", label the information "CalHR Internal User Only" or you may choose to use other similar labels that convey the appropriate increasing level of sensitivity and confidentiality. The additional label "3rd Party Confidential" may also be used if appropriate.

Access: CalHR employees and non-employees with signed confidentiality agreement.

Distribution within CalHR: Standard interoffice mail, approved e-mail and electronic file transmission methods.

Distribution outside of CalHR internal mail: U.S. mail and other public or private carries, approved e-mail and electronic file transmission methods.

Electronic distribution: No restrictions to approved recipients within the Department, but this material should be encrypted or sent securely if being sent to approved recipients outside of CalHR premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on CalHR premises.; electronic data must be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution.

4.3 Most Sensitive: This category includes operational, personnel, source code, personal identifiable information, medical and psychological Records, and otherwise privileged material.

4.3.1 Designation of Material in Hardcopy or Electronic Form.

There is no requirement to mark CalHR Confidential Information, but users should be aware that this information is very sensitive and must be protected as such. To indicate CalHR Confidential Information is very sensitive, we recommend labeling the information "CalHR Internal: Registered and Restricted", "CalHR

Eyes Only", "CalHR Confidential" or similar labels at the discretion of your individual business unit or department. *Any of the markings above may be used with the additional label "3rd Party Confidential".*

Access: Only those individuals (CalHR employees and non-employees) designated with approved access and signed confidentiality agreement.

Distribution within CalHR: Delivered direct – signature required, envelopes stamped confidential, or approved e-mail and electronic file transmission methods.

Distribution outside of CalHR internal mail: Delivered direct; signature required; approved private carriers; encrypted/secure e-mail and electronic file transmission methods.

Electronic distribution: No restrictions to approved recipients within CalHR, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secure computer.

Disposal/Destruction: Strongly Encouraged; In specially marked disposal bins on CalHR premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination and possible civil and/or criminal prosecution.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

Terms and Definitions

Approved Electronic File Transmission Methods

Includes supported File Transfer Protocol (FTP) and Web browsers.

Approved Electronic Mail (e-mail)

Includes all mail systems supported by the Information Technology Division (ITD). These include, but are not necessarily limited to Outlook. If you have a business need to use other e-mail providers, contact the helpdesk.

Approved Encrypted e-mail and files

Encryption is available via many different public domain packages on all platforms. These domain packages include Data Encryption Standard (DES) and Pretty Good Privacy (PGP).

Delivered Direct; Signature Required

Do not leave in interoffice mail slot; call the mail room for special pick-up of mail.

Envelope Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it and stamp it confidential.

Individual Access Control

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner.

SECURITY INCIDENT REPORTING

1.0 Overview

This policy outlines how to identify and report information security incidents.

2.0 Policy

The California Department of Human Resources ("Department" or "CalHR") must promptly investigate incidents involving loss, damage, misuse of information resources, or improper access or distribution of information.

2.1 Incident Reporting

An essential part of information security responsibilities is to report known or suspected information security incidents that may place the Department's information resources at risk.

2.1.1 Identifying an Information Security Incident

In order to maintain good information security, authorized users must recognize and report information security incidents promptly to CalHR's Information Security Officer (ISO) or Chief Information Officer (CIO). Authorized users must be alert to incidents that could expose confidential, sensitive, or personal information to unauthorized access, use, disclosure, modification, or destruction.

The following are some examples of incidents to report:

Theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, personal digital assistants (PDA), smart phones or any electronic devices that may contain or store confidential, sensitive, and/or personal data.

Loss or theft of State data that includes electronic or paper records, or any other medium (e.g. tape, optical disk).

Mailing documents containing personal information to the wrong person.

Hacking into State computer systems.

Successful virus attacks, Web site defacements, server compromises, and denial of service attacks.

Unauthorized, inappropriate, or illegal use of network systems, computer software, or equipment.

Intentional or unintentional release of personally identifiable information (PII).

2.1.2 Reporting an Information Security Incident

When an incident or potential incident is detected, authorized users must immediately notify the Department ISO and/or the authorized user's immediate supervisor.

Depending on the type of incident and the information involved, CalHR's ISO must immediately call the California Highway Patrol's (CHP) Emergency Notification and Tactical Alert Center (ENTAC).

If the information security incident involves potential unauthorized access to unencrypted personal information, State policy and law require CalHR to promptly notify the affected individual(s) in writing of the security breach, in addition to notifying CHP as described above.

3.0 Terms and Definitions

Information Resources

All categories of automated information, including (but not limited to) records, files, and databases.

Personally Identifiable Information (PII)

An individual's first name or first initial and last name in combination with at least one of the following:

Social Security number

Driver's license or California ID card number

Financial account number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Medical/psychological information

Health Insurance Portability and Accountability Act (HIPAA) information

Authority
Civil Code Section 1798.29
Government Code Section 11549
Government Code Section 14613.7(a)
State Administrative Manual Section 5350
Information Security Notification and Reporting, Budget Letter 06-34

PORTABLE COMPUTING DEVICES AND PORTABLE ELECTRONIC STORAGE MEDIA

Overview

Mobile computing has become an inherent part of doing business. Most portable computing devices and portable electronic storage media have the capacity to store departmental data. In addition, portable devices and portable storage media are well-known source of malware infections. Because data can be portable and is one of the causes of malware infection, CalHR must exercise due diligence to ensure data is appropriately protected.

Policy

This policy applies to all authorized users who use portable computing devices or portable electronic storage media, including department-owned, employee-owned, or contractor-owned to access, transmit, or store State data that is confidential, sensitive, or personal.

All portable computing devices or portable electronic storage media owned by the Department will have the Department's encryption software standard installed prior to use.

All purchases of portable computing devices or portable electronic storage media will include the purchase of the approved Department's encryption software standard license or encryption software subject to approval by the Information Technology Non-Standard Software guidelines.

Non-departmental portable computing devices and portable electronic storage media (i.e., devices belonging to contractors or other entities) are not allowed to connect to CalHR's network without prior authorization from the Department Information Security Officer (ISO) or Chief Information Officer (CIO).

All portable computing devices or portable electronic storage media will be password protected to safeguard from incidental unauthorized access. (See Password Policy.)

Portable computing devices and portable electronic storage media owned by authorized users are automatically encrypted upon initial connection to CalHR's network.

Terms and Definitions
Mobile Computing

Is a generic term describing one's ability to use technology "untethered" which means the device does not need a cable to connect to a network.

Portable Computing Devices

These include, but are not limited to Personal Digital Assistants, notebook computers, Tablet Personal Computers (PC), Palm Pilots, Microsoft Pocket PCs, Blackberry devices, audio/video players, text pagers, smart phones, and other similar devices.

Portable Electronic Storage Media

This includes, but is not limited to compact discs (CD), Digital Video Disc (DVD), memory sticks, universal serial bus (USB) drives also known as thumb or flash drives, floppy disks, and other similar devices.

Authority

Encryption of Portable Computing Devices, Budget Letter (BL) 05-32

CLEAN DESK POLICY

1.0 Overview
The purpose of this policy is to establish a culture promoting information security by encouraging all California Department of Human Resources ("Department" or "CalHR") employees, contractors, students and volunteers to be aware of and take steps to limit access to documents on their desks.

2.0 Purpose
This clean desk policy:
Produces a positive image when non-Department people visit the Department and demonstrates CalHR's commitment to information security.
Reduces the threat of a security incident.

3.0 Scope
This policy applies when an employee leaves their desk such as when attending meetings and on breaks. During these times, sensitive working papers and media should be placed in locked drawers. At the end of the day, documents on the desks should be organized and all papers and media with confidential or sensitive data should be locked in filing cabinets or otherwise secured.

4.0 Policy
The following practice should be followed to ensure a clean desk:

Allocate time in your calendar to organizer paperwork or media.

Always clear your workspace before leaving for extended periods (i.e. going to a meeting, leaving for the night, going on vacation).

If in doubt – throw it out. If you are unsure whether a duplicate piece of sensitive or confidential documentation should be kept – it will probably be better to place it in the shredder or shred bin.

Discard sensitive or confidential documents securely when they are no longer needed.

Always lock your desk and filing cabinets that contains sensitive and confidential information.

PRINTER POLICY

1.0 Overview

Printers represent one of the highest equipment expenses at the California Department of Human Resources ("Department" or "CalHR"). The goal of this policy is to facilitate the appropriate and responsible business use of CalHR's printer assets, as well as to control CalHR's printer costs.

2.0 Policy

Printers are to be used for documents required to conduct CalHR's business. CalHR printers should not be used to print personal documents except where specified in the Incidental Use section of the Acceptable Use Policy.

Individual personal printers are not recommended and are not generally approved because of maintenance and support costs. However, in certain circumstances, however, such as remote locations or other unusual situations, personal printers may be allowed.

Do not use the printer to print multiple copies of the same document. Decrease production costs by printing one copy on the printer and use the photocopier to make additional copies.

Pick up printed material in a timely fashion. If you no longer want the document(s), dispose of the material appropriately consistent with its level of confidentiality.

If there is unclaimed material on the printer, stack it neatly next to printer. All unclaimed material left by the printer will be discarded after 3 days.

If possible, limit paper use by taking advantage of duplex printing (i.e. double-sided printing) features offered by most CalHR printers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).

Make efforts to limit toner use by selecting light toner and lower dots per inch(dpi) default print settings.

Avoid printing large files. This puts a drain on network resources and interferes with the ability of others to use the printer. Report any planned print jobs in excess of 100 pages to the IT department so that the most appropriate printer can be selected and other users can be notified.

If printing material in excess of 25 pages, position yourself at the printer to ensure adequate paper supply and to ensure the output tray is not overfull.

Avoid printing e-mail messages. Use the folders and archiving function in your e-mail application to organize and view your messages.

Avoiding printing a document just to see what it looks like. Use Print Preview.

Do not re-use paper in laser printers because this can lead to paper jams.

Before using certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper, consult with IT to learn which machines can handle these special papers.

Avoid printing in color when monochrome (black) will do.

Printer paper is available in Business Services. Toner cartridges are available through the helpdesk.

If there is a problem with the printer (paper jam, out of toner, etc.) and you are not “trained” in how to fix the problem, please do not try. Instead, report the problem to the Help Desk or ask a trained co-worker for help. Report any malfunction of any printing device to the helpdesk as soon as possible

SOCIAL MEDIA

1.0 Overview

Social Media can be a useful way to communicate and promote the exchange of ideas. However, use of social media also presents certain risks and carries with it certain responsibilities.

2.0 Definition

Social Media is an electronic service or account, or electronic content, including but not limited to videos, still photographs, blogs, video blogs, podcasts, instant and text message, email, online services or accounts, or Internet Website profiles or locations. This includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else’s web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board, commercial web site or a chat room, whether or not associated or affiliated with the State and whether or not accessed through State issued or personal electronic equipment, as well as any other form of electronic communication. Some examples of Social Media websites include Facebook, Twitter, Blogger, or You Tube.

3.0 Policy

3.1 Accessing Social Media Websites at Work

CalHR employees should refrain from using Social Media at work, while on state time or while using state equipment, unless the employee has been authorized by management to access such sites in accordance with departmental and state policies. Even where authorized, use of social media in the workplace using state equipment should be on a minimal and incidental basis.

3.2 Posting Information On Behalf of the State

CalHR employees should not speak in Social Media web sites or other on-line forums on behalf of CalHR unless specifically authorized by CalHR's Director or CalHR's Public Information Office. CalHR employees who are authorized to speak on behalf of the department shall identify themselves by name, title, department and contact information, and shall only address those issues within the scope of their specific authorization.

3.3 Posting information about CalHR or CalHR employees

CalHR employees should use caution to ensure that opinions expressed through social media are readily identifiable as their own personal opinions and do not represent the position of the State or an agency or CalHR. It is best to include a disclaimer such as, "The postings on this site are my own and do not necessarily reflect the views of CalHR." CalHR employees who post such information on social media should exercise due care to ensure that their communications are fair and courteous to their fellow employees, other state workers, and members of the public with whom they interact in the course of their employment.

3.4 Communicating About the Terms and Conditions of Employment

CalHR employees engage in concerted and protected activity when they use Social Media to communicate with one another about work-related issues such as workload, staffing, employment conditions and wages. Posts that are not work-related or that express individual personal gripes or disputes are generally not considered concerted and protected activity.

3.5 Information That Should Not Be Posted

CalHR employees are solely responsible for their postings. CalHR employees should ensure that their postings are consistent with the department's internal policies such as policies governing Discrimination and Harassment Prevention, Workplace Violence Prevention, and Incompatible Activities. Postings that include discriminatory and/or harassing remarks, threats of violence, or similar inappropriate conduct directed to or concerning other state employees, their employer or stakeholders who have a nexus to their employment violate such policies. In addition, CalHR employees should not post or release proprietary, confidential, sensitive, privileged or other state government intellectual property. Confidential information can include internal departmental reports, policies, procedures or attorney-client communications, doctor-client communications or other internal communications. For example, information related to advice received regarding pending litigation against CalHR, or the Social Security and/or driver's license numbers of members of the public which a CalHR employee obtains during the course of his/her duties as a CalHR employee cannot be posted on any Social Media.

3.6 Examples of Inappropriate Postings

Inappropriate postings can include discriminatory remarks, harassment and threats of violence which violate CalHR's policies and concern other state employees or have some other nexus to your workplace, CalHR or your employment with CalHR. In posting information or material which concerns other state employees or CalHR, CalHR employees should avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening, intimidating, disparaging, defamatory, harassment or bullying, or invading another's right to privacy. CalHR employees should also avoid offensive posts meant to intentionally harm someone's reputation or posts that contribute to a hostile work environment on the basis of race, sex, sexual orientation, age, disability, religion or any other protected status.

4.0 Possible Disciplinary Action

Inappropriate postings, as defined above, and those postings that violate CalHR or State laws or policies will not be tolerated and may subject employees to disciplinary action up to and including termination.

5.0 No Retaliation

Retaliation against an employee who reports another employee for posting inappropriate postings, as defined above, or for cooperating in an investigation into such alleged postings is prohibited.

6.0 Deleted Postings

The internet archives everything; even deleted postings can be accessed. Ultimately, employees are solely responsible for their postings.

7.0 Questions

If a CalHR employee has a question about any part of this policy, the employee's immediate supervisor should be contacted.

PHYSICAL AND ENVIRONMENTAL

1.0 Overview

Physical and environmental security refers to measures taken to prevent unauthorized access and damage to information resources, buildings and related supporting infrastructure associated with their physical environment. The practices must be adequate to protect the most sensitive information technology application located within the physical location of the California Department of Human Resources ("Department" or "CalHR").

2.0 Policy

This policy establishes the requirements for physical and environmental security to protect information resources, system resources and the physical environment itself used to support the Department's operation. The Department director or the designee must take appropriate measures as follows:

Provide management control of physical access to information resources (including personal computer systems, computer terminals, and mobile devices) by agency staff and outsiders. (See Password Policy)

Secure areas to be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Prevent, detect, and suppress fire, water damage, vermin, civil unrest and other forms of natural or man-made disaster.

Protect, detect, and minimize loss or disruption of operational capabilities due to electrical power fluctuations or failure.

Use security perimeters to protect areas that contain information-processing facilities.

All systems, storage media, and network components that are State-owned or owned by other external entities providing CalHR services must be physically secured so that access is restricted to personnel authorized by the Data Owner.

Provide management control of physical access to the work site as follows:

Visitors – All visitors must arrive at the designated Check-In entrance and must be met by their employee sponsors at the time of Check-In.

Forgotten Badges – An authorized user who forgets their badge will need to obtain a temporary badge from Business Services. This badge will expire at the end of the day in which it is obtained. The temporary badge needs to be returned to Business Services either at the end of the day or the following business day.

Lost Badges – When an authorized user loses their badge, they must report the loss to Business Services immediately. The authorized user must obtain a new badge by paying the necessary fee in Accounting. Accounting will notify Business Services the fee has been paid and Business Services will then issue the authorized user a new badge.

3.0 Authority

Government Code Section 11549
Government Code Section 14685(c)(1)
State Administrative Manual Section 5330
ACCESS CONTROLS

Overview

Access controls authenticate a user's identity, establish accountability, and reduce unauthorized system access risks. User identification (ID) and passwords are a form of access control. Access control is a method for managing system availability, accessibility through authentication (Who are you?), and authorization (What rights do you have?). Access control ensures protection of information resources entrusted to the California Department of Human Resources ("Department" or "CalHR") and is often administered at different levels such as through the personal computer (PC), database (dB), Local Area Network (LAN), and Wide Area Network (WAN).

Policy

This policy addresses the physical, technical, and administrative controls necessary to support proper access to the Department's information resources. These controls must be based on both business and security requirements to prevent and detect unauthorized access and must, at a minimum, include the following controls:

Mobile and Telework Access – Mobile and telework access controls include, but are not limited to the following:

Identifying computing systems that allow dial-up communication or Internet access to confidential, sensitive, or personal information, and information necessary for the support of agency critical applications.

Periodically changing dial-up access telephone numbers.

Auditing usage of dial-up communications and Internet access for security violations.

Controlling remote access connectivity requires the following:

All remote access connections must come through the Department's approved remote access entry points.

Remote access users connecting to the Department's network must adhere to department policies and processes to obtain approval.

Remote access sessions will be monitored and logged and employ session time limits (active idle).

Remote access sessions utilizing the Internet as the means of connectivity must be encrypted (e.g. Virtual Private Network (VPN) Client, Secure Socket Layer (SSL)).

The telephone numbers used on incoming modem lines must not be published in any directory that may be accessed by anyone other than those authorized for access.

Wireless connectivity requirements are as follows:

Private Access:

Users connecting to the Department's network using wireless access must adhere to department policies and processes to obtain approval.

Users connecting to wireless access must use approved devices with 802.1X encrypted authentication and authorization.

Public Access:

Approved Users utilizing the Department's wireless connections must have prior authorization via ITD helpdesk.

Connections from the approved user's device must be made through an authenticated connection.

Any place there is an entry point to the Department's network, there must be an appropriate level of authorization for the data streams entering or leaving. In addition, there must be additional authorization prior to accessing network resources used for creation, modification, retrieval, or storage of data.

The act of logging in is similar to the act of going through the front gate or door. This is where the users or services identify themselves and present some type of credentials to request entry.

Log-in services must provide for positive authentication, which will ensure that an authorized user is allowed access to the system or network environment.

Authorized users must log off and/or secure workstations with a password protected screen saver when not in use.

Managers, supervisors or designated employees are responsible for defining the appropriate level of authorization for their authorized users. Users and services must be granted rights and privileges only on a "need to know" or only on a need-to-use basis and according to the principle of "least privilege."

Network administrators must ensure that unused workstations are secured by "log off" or other means when they remain idle for 10 minutes.

Non-Authorized Users

Non-Authorized Users (i.e. contractors, visitors, etc.) must be given access to the network and its resources by a department sponsor utilizing appropriate forms as necessary.

User I.D. must be assigned only for the duration that access is required. User I.D. must be revoked following the end of the access requirement.

Special Privileges

Procedures for special privileges must be written by the Information Technology Division (ITD) together with the Information Security Officer (ISO) to ensure that they can be administered properly within the Department's technical environment. These procedures must define how access requirements will be administered, managed, and reviewed.

The Department has the right to revoke any authorized user's access privileges for violations of this policy or conduct that disrupts the normal operation of the Department's network and computing systems.

Terms and Definitions

Access

The ability, right, or permission to view, modify, or communicate information.

Access Control

Access controls grant or deny an individual permission to access all or part of a data resource. They help ensure that authenticated individuals or devices can perform operations only on the system resources for which they are authorized. The business rules within each application must identify what data a particular authenticated individual may view, and what operations (read, write, modify, or delete) the individual may perform.

Authentication

The process of determining whether someone who or something is, in fact, who or what it is declared to be. Authentication is often a prerequisite to allowing access to network resources.

Authorization

The granting of privileges in accordance with legal authority and the business needs of the requester to an individual, a program, or a process to allow access to an information resource.

Data Stream

A continuous flow of information or data.

Local Area Network (LAN)

Two or more personal computers connected by cable, telephone wire, or other communication facility, at the same site, providing the ability to communicate or to access shared data storage, printers or other personal computer commodities.

Remote Access

The ability to log onto a network from an off-site location. Generally, this implies a computer, a modem, and some remote access software is used to connect to the network.

Special Privileges

Refers to the use of special system accounts (commonly known as root, administrator, etc.) for operating systems and software applications.

Secure Sockets Layer (SSL)

SSL is an open standard that combines public key technology and symmetric encryption to provide authentication, confidentiality, and message integrity to network or Internet transactions.

Telework

California Government Code Section 14200 states telework or “telecommuting” means “the partial or total substitution of computers or telecommunication technologies or both, for the commute to work by employees residing in California.”

Virtual Private Network (VPN)

A private network that is configured within a public network in order to take advantage of the economies of scale and management facilities of large networks. VPNs are widely used to enable mobile and remote users to connect to their company’s internal LANs.

Wide Area Network (WAN)

A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more LANs.

Wireless

Computer networking, broadcasting, telephony, or telegraphy using radio signals/electromagnetic waves to send and receive data instead of wires.

Authority

Government Code Section 11549

State Administrative Manual Section 5340

NETWORK BANNER

Overview

Network Banners are information presented to users prior to allowing access to a computer network or system. Notification serves as an electronic “No Trespassing” sign. Network Banners can contain information about the system or company, legal consequences for unauthorized access, and define rules of conduct. Network Banners advising who can use the system constitute non-disclosure statements.

Policy

All entry points to the California Department of Human Resources’ (“Department” or “CalHR”) network must display the network banner contained in Section 3.0.

Network Banner

All computing devices that connect to the Department’s network are subject to displaying the Department’s network banner.

The Department’s Network Banner displays as follows:

WARNING!

WARNING: This is a State of California computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY, if you are not an authorized user or you do not agree to the conditions stated in this warning.

Disabling of the Department’s network banner is prohibited.

Any modification to the Department’s network banner is prohibited.

INTERNET (WEB) MONITORING

Overview

The Internet is a public network utilized by companies, government agencies and the general public. Systems that connect to the Internet have the exposure of being “seen” by any other system on it. This exposure is the entry point where attackers are looking to gain access to perform attacks.

Internet attacks and the variety of methods used to perform these attacks have increased. Malicious codes, phishing, internet browser, and operating system exploits using spyware, crime ware, and keystroke logging installations are some of the methods used by attackers. The California Department of Human Resources ("Department" or "CalHR") must ensure the needed protection is in place.

To prevent internet attacks and protect the Department's information resources, the Department implements a solution which involves hardware and software installations that identify and block known websites or Internet Protocol (IP) addresses that are associated with methods used by attackers to perform exploits or that contain inappropriate content. These known websites evolve and change almost daily. Therefore, the ability to completely and permanently ensure an unsuccessful attack or inappropriate content is not practically possible.

Policy

The Information Technology Division (ITD) as data custodians must implement and maintain a web security solution that protects it from existing and emerging web-based threats.

2.1 Web Site Monitoring

The ITD monitors Internet use from all computers and devices connected to the Department network. For all traffic, the monitoring system must record the source IP Address, the date, the time, the protocol, and the destination site or server. Where possible, the system must record the User ID of the person or account initiating the traffic. Internet Use records must be preserved for at least 90 days.

2.2 Internet Use Filtering System

Internet filtering allowing approved content must be applied to all Internet traffic coming into the network. Users attempting to connect to known unapproved websites or content will be denied access.

The ITD will block access to Internet websites and protocols that are deemed inappropriate for CalHR's environment. The following protocols and categories are examples of websites that must be blocked:

Adult/Sexually Explicit Material

Gambling

Hacking

Illegal Drugs

Peer to Peer File Sharing

Personal Cloud storage (online storage)

Personals and Dating

Spyware

SPAM, Phishing and Fraud

Tasteless and Offensive Content

Violence, Intolerance and Hate

Other Offensive Contents

2.2.1 Web Monitoring Filter Changes

The ITD must periodically review and recommend changes to web and protocol filtering rules. Personnel Services Division will review the recommendations and decide if any changes are to be made.

2.2.2 Web Monitoring Filtering Exceptions

If a site is miscategorized, employees may request the site be unblocked by submitting a help desk ticket. The help desk will review the request and unblock the site if it is miscategorized.

Employees may access a blocked site with permission if appropriate and necessary for business purposes. The employee must submit a request to their immediate supervisor who will then present it to help desk. ITD will unblock the site or category for that associate only. ITD must track approved exceptions and report on them upon request.

2.3 Reports

General trending and activity reports will be periodically made available and distributed to executive management.

2.4 Department Banner

Attempting to access a website that has been blocked by the internet filtering system will display the message below.

“The URL you requested has been blocked by the URL Filter database module of MCAfee Web Gateway. The URL is listed in categories that are not allowed by your administrator at this time. This was blocked using the XXXXX Policy.”

Note**:** XXXXX represents the category or filter that was triggered.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Terms and Definitions

Crime Ware

Any computer program or set of programs designed expressly to facilitate illegal activity online.

Internet Protocol (IP) Address

Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

Keystroke logging (a.k.a. Key Logging)

A diagnostic tool used in software development that captures the user's keystroke. When software using a key logger method records the information typed into a system or application to capture information, such as usernames and passwords for the purpose of obtaining information to spy on computer usage, this is known as a form of malicious code.

Malicious Code

Malicious code includes any and all programs (including macros and scripts) which are deliberately coded in order to cause an unexpected (and usually, unwanted) event on a user's personal computer.

Peer to Peer File Sharing

Services or protocols such as Bit Torrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts.

Personal Cloud Storage

An online web service that provides server space for an individual to store data, photos, videos and other files which allows an individual access to that data from anywhere.

Phishing

The practice of luring unsuspecting Internet users to a fake Web site by using authentic-looking e-mail with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack.

SPAM

Unsolicited internet e-mail. SPAM sites are websites that link to unsolicited internet mail messages.

Spyware

Any software that covertly gathers information about a user while he/she navigates the Internet and transmits the information to an individual or company that uses it for marketing or other purposes.

Authority

Government Code Section 11549
State Administrative Manual Section 5320.3
Protection of Information Asset, MM 06-12

MALWARE

Overview

Malicious computer software, such as viruses, worms and Trojan Horses are software with the intent to cause harm. The short term for malicious software is "malware." If malicious software is spread and infects the California Department of Human Resources' ("Department" or "CalHR") networks, it not only costs time and money in remediation, but also lowers productivity. The spread of malware infections throughout the Department and to its partners that connect to our network could adversely impact the Department's mission and goals.

Policy

The Department data custodians, Information Technology Division (ITD), must use all means to prevent the spread of malware among its networked systems. Users must not circumvent anti-virus software in any way.

All systems must have Department approved anti-virus protection software tools installed before connecting to the network.

All workstations and servers are to maintain active anti-virus protection.

Authorized users must participate in keeping anti-virus software updated and must not turn off or disable anti-virus protection systems.

Any files obtained from sources outside the Department's network, including disks brought from home, files downloaded from the Internet, files attached to e-mail, files provided by customers or vendors, and other online services, including but not limited to newsgroups, bulletin boards, etc… will be scanned automatically upon initial access using Department resources.

Third party software must be scanned prior to installation on networked computers.

In the case of a possible incident, call the ITD help desk at 916-327-0520 for immediate attention and report any incident to the Department Information Security Office.

Terms and Definitions

Anti-Virus Software

Software designed to prevent, detect and remove most malicious software (malware).

Malware

Software such as viruses, worms, and Trojan horses with the intent to cause harm. Malware interferes with normal computer functions or sends personal data about the user to unauthorized parties over the internet.

DISASTER RECOVERY

Overview

Disaster recovery planning provides for continuity of computing operations in support of critical business functions; facilitates orderly, preplanned responses to incidents; produces the greatest benefit from remaining limited resources and, achieves a systematic and orderly migration toward the resumption of all computing services within an agency following a business disruption.

Policy

2.1 Disaster Recovery Plan Contents

The California Department of Human Resources ("Department" or "CalHR") must maintain a Disaster Recovery Plan (DRP) and must be reviewed annually to assure its relevance.

A DRP must:

Identify critical business functions.

Identify business impact and risk based on analysis.

Identify maximum acceptable outage for each critical business function

Provide procedures to cover prolonged unavailability of critical information resources, communications services, personnel, buildings or access to buildings.

Provide procedures to cover unavailability of services provided by state data center or third party service provider.

Support the Department's other emergency plans, such as, the Continuity of Operations/Continuity of Government (COOP/COG), Emergency Operations Plan (EOP), and other Departmental Emergency Plans.

Must cover at least ten topic areas which are listed and described in the Disaster Recovery Plan Documentation for Agencies Preparation Instructions (SIMM Section 65A).

2.2 Requirements for Disaster Recovery Plans

The Department must keep its DRP up-to-date and provide annual documentation for those updates to the California Office of Information Security (OIS). These annual requirements are as follows:

The Department must file a copy of its DRP and the Agency Disaster Recovery Plan Transmittal Letter (SIMM Section 70D) with OIS, in accordance with the Agency Operational Recovery Plan Submission Schedule.

If the Department employs the services of a State data center, it must also provide the data center with either a full copy or a subset of its plan, containing enough information for the data center to recover the agency's systems and/or data.

The Department may file an Agency Disaster Recovery Plan Certification (SIMM 70B) in place of a full DRP, if both of the following conditions exist:

A full plan was submitted the previous year and is on file with the OIS.

No changes are needed to the current plan.

Terms and Definitions

State Data Center

Provides information technology services to many state, county, federal and local government entities throughout the State.

COOP/COG

Enables agencies to continue their essential functions across a broad spectrum of emergencies in support of an enduring constitutional government.

Authority

Government Code Section 11549

State Administrative Manual Section 5355

Changes to Operational Recovery Planning, Budget Letter 07-03

PASSWORDS
1.0 Overview
Authentication is the process of proving that users are who they say they are. Passwords along with user identifications (ID) are an important part of authentication in the security of all information resources. Password requirements that are too complex can cause excessive password resets or cause users to record them creating an increased risk of compromise. Passwords that are too simplistic can defeat the level of security.

Accordingly, passwords must, wherever technologically possible, comply with rules that enforce strong controls that limit exposure to guessing, brute force attacks, and password cracking tools.

Authenticating to multiple systems result in multiple passwords for the user. Single sign-on (SSO) technology enables a user to authenticate once and gain access to the resources of multiple software systems. SSO capability is highly desirable, but does not negate the need to maintain secure systems through good authentication practices.

2.0 Policy
This policy establishes the requirements for passwords and the protection of those passwords. All authorized users are responsible for the confidentiality and security of their passwords.

The following password protection requirements must be met to secure data from unauthorized access:

Shared passwords are prohibited since they do not provide specific accountability. Generic or group passwords shall not be used.

Passwords are to be changed immediately if revealed or compromised.

Automated scripts that defeat password controls are prohibited.

Automated scripts, including but not limited to, workstation logon, server or program authentication is prohibited.

Authorized User Passwords must meet the following criteria:

Must be at least eight (8) characters long.

May not contain your login user name or any part of your full name.

May not be a single dictionary word.

Passwords must contain characters from at least three (3) of the following four(4) classes.

Table 1 Authorized User's Password Classes

Character Classes	Character Example
upper case letters	A, B, C, …Z
lower case letters	a, b, c, … z
numerals	0, 1, 2, …
non-alphanumeric “special characters”	punctuation marks and other symbols

Table 2 Authorized User's Password Requirements

Account Policy	Requirements
Password History	12 passwords
Maximum Password Age	90 days or less
Minimum Password Age	1 day
Minimum Password Length	8 characters
Maximum Password Length	Depends on the limitations of the system, but should be at least 25
Account Lockout Threshold	3 attempts
Maximum Grace Period	14 days

System User Passwords must meet the following criteria:

Must be at least eight (8) characters long.

May not contain your login user name or any part of your full name.

Must be changed by the user at the next logon whenever it is reset.

Passwords must contain characters from at least three (3) of the following four(4) classes:

Table 3 System User Password Classes

Character Classes	Example
upper case letters	A, B, C, …Z
lower case letters	a, b, c, … z
numerals	0, 1, 2, …
non-alphanumeric “special characters”	punctuation marks and other symbols

Table 4 System User Password Requirements

Account Policy	Requirements
Password History	12 passwords
Maximum Password Age	60 days or less
Minimum Password Age	1 day
Minimum Password Length	8 characters
Maximum Password Length	Depends on the limitations of the system, but should be at least 25
Account Lockout Threshold	3 attempts
Maximum Grace Period	14 days

***Administrative* and *Service Account* Passwords** must meet the following criteria:

Must be at least twelve (12) characters long

May not contain your login user name or any part of your full name.

Passwords must contain characters from at least three (3) of the following four(4) classes:

Table 5 Administrative and Service Account Password Classes

Character Classes	Example
upper case letters	A, B, C, …Z
lower case letters	a, b, c, … z
numerals	0, 1, 2, …
non-alphanumeric “special characters”	punctuation marks and other symbols

Table 6 Administrative and Service Account Password Requirements

Account Policy	Requirements
Password History	12 passwords
Maximum Password Age	365 days or when position is vacated
Minimum Password Age	1 day
Minimum Password Length	12 characters
Maximum Password Length	Depends on the limitations of the system, but should be at least 25
Account Lockout Threshold	3 attempts
Maximum Grace Period	14 days

Terms and Definitions

Administrative Account

An account that is granted express, implied or apparent authority to use the information resources and make changes to them.

Account Lockout Threshold

Determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired.

Authorized User

Any person granted express, implied or apparent authority to use any information resources available on the network.

Automated Scripts

A series of programming commands that run uninterrupted without user intervention.

Brute Force Attack

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN).

Maximum Grace Period

Determines the number of times a user can login prior to the expiration of their password. Once the password expires, the account is locked and needs to be reset by an administrator.

Maximum Password Age

The period of time (in days) a password can be used before the system requires the user to change it.

Maximum Password Length

The most number of characters a user account password may contain.

Minimum Password Age

The period of time (in days) a password must be used before the user can change it.

Minimum Password Length

The least number of characters a user account password may contain.

Password History

The number of unique new passwords that have to be associated with a user account before an old password can be reused.

Reset

Changing a password due to expiration, lock-out or program enforcement.

Service Account

Accounts used by applications to interface with other applications/resources. (For example: an account that is used by an application to access a database resource)

User Account

User accounts used to establish trust between an end user and applications/resources. (For example: user account for the state application or savings plus program)

RISK MANAGEMENT

Overview

Risk management is the process of identifying, assessing, and responding to the risks associated with information resources through a risk analysis process.

A risk management program is an essential management function that is critical to the implementation and maintenance of an acceptable level of security. The risk management program will help the California Department of Human Resources (“Department” or “CalHR”) identify, assess, and respond to the risks associated with its information resources. The program will also preserve the department’s ability to meet its program objectives in the event of the unavailability, loss, or misuse of information resources.

The risk management program enables the Department to accomplish its mission by (1) securing the Information Technology (IT) systems and processes that store, manipulate, or transmit department information; (2) enabling management to make well-informed risk management decisions; and (3) assisting management in authorizing and/or acquiring systems or processes on the basis of risk management results.

Policy

The Information Security Officer (ISO) is responsible for developing policies that define and govern the risk management program, and is responsible for evaluating and ensuring the department's compliance with the risk management program. The risk management program must include three main processes: risk analysis, risk mitigation, and ongoing evaluation.

Deputy Directors, Division Chiefs, Program Managers, Office Managers, and Supervisors are responsible for:

Ensuring authorized users are informed and abide by this policy.

Immediately reporting loss of integrity of computerized information resources to the Department's Information Security Officer.

Authorized users, including all department employees, contractors, student assistants, and volunteers are required to:

Adhere to this policy.

Immediately report loss of integrity of computerized information resources to the Department Information Security Officer or, if the ISO is not accessible, to the employee's immediate supervisor.

Risk Analysis

The risk analysis process must be completed through a comprehensive risk analysis cycle at least every two years and whenever there is a significant change in the use of information technology. The risk analysis process will consist of:

Identification and assessment of risks associated with information resources, and defining a cost-effective approach to manage such risks. Specific risks that must be addressed include, but are not limited to:

Accidental and deliberate acts on the part of department employees and outsiders.

Fire, flooding, and electric disturbances.

Loss of data communications capabilities.

Identification and prioritization of critical applications of information technology.

Preparation of a risk assessment report.

Risk Mitigation

The risk mitigation process must prioritize, evaluate, and implement the appropriate risk-reducing controls based on the risk assessment report.

Ongoing Evaluation

The risk analysis must be conducted on a regularly scheduled basis at least bi-annually or when changes occur to the Department that would constitute a re-evaluation. (i.e. office relocation)

Terms and Definitions

Critical Applications

A function that is so important to the state that the loss or unavailability of the function is unacceptable.

Information Resources

All categories of automated information, including (but not limited to) records, files, and databases.

Risk Analysis Process

The steps taken to identify the risks to system security and to determine the probability of occurrence, the resulting impact, and the additional safeguards that would mitigate this impact.

Risk Management

The process of identifying, controlling, and mitigating information system-related risks. This process includes both the identification and assessment of risks through risk analysis, and the initiation and monitoring of appropriate practices in response to these analyses.

Authority

Government Code Section 11549

State Administrative Manual Section 5305

Agency Risk Management and Privacy Program Compliance Certification Requirements, Budget Letter 06-34

SOFTWARE COPYRIGHTS
Overview

A copyright is the exclusive legal right to reproduce, publish, and sell a piece of intellectual property. A software license is a license to use the software by a specific device or by a specific number of users. Computer software can be copyrighted and licensed.

Software piracy refers to the installation or use of unlicensed or unauthorized copies of software.

Policy

Only software that has been legally acquired and licensed by the California Department of Human Resources ("Department" or "CalHR") may be used on department owned or leased equipment.

Users may not copy material protected under copyright law or make that material available to others for copying.

Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, images, graphics, documents, messages, and other material that can be downloaded or copied.

Terms and Definitions

Intellectual Property

Property that results from original creative thought, such as patents, copyright material, and trademarks.

Software License

A license to use the software by a specific resource or by a specific number of users.

Authority

Government Code Section 11549

State Administrative Manual Section 5345.1

STATE LICENSED SOFTWARE ON NON-STATE IT EQUIPMENT

Overview

Software integrity practices ensure all software must be fully licensed and obtained only from a reputable source. Computer software management practices ensure that computer software in use is legally procured and is used in compliance with licenses, contract terms, and applicable copyright laws.

Policy

To ensure software licensed to the California Department of Human Resources ("Department" or "CalHR") is tracked and accounted for, the Information Technology (IT) Division's Software Management Plan together with the Contractors Certification procedures must exist.

Computers with Department-funded software will be included in the ongoing software inventories and internal audits. Any audit of non-state equipment running Department-licensed software will not include a review of the personal files of the employee, and will be limited to CalHR business information.

Contractors Certification

The IT Resource Management Office staff will ensure all new IT contracts with the department include the necessary software compliance language.

Every department contractor will have a signed certification of State-licensed software compliance on record with the department.

The department contract owner, i.e. the person responsible for the work the contractor is performing, will be responsible on an ongoing basis to make sure the contractor remains in compliance.

IT will assign support staff to monitor software usage and monitor adherence to policies and procedures.

Definitions

Software License

A license to use the software by a specific device or by a specific number of users.

Authority

Government Code Section 11549

State Administrative Manual Section 5345.1

SYSTEMS DEVELOPMENT AND MAINTENANCE

1.0 Overview

The California Department of Human Resources ("Department" or "CalHR") develop systems that are available for public and state agency use. Since the CalHR systems also house sensitive data that are accessed via the internet, applications developed must provide security and data integrity.

2.0 Purpose

The purpose of this policy is to define requirements for system security planning and management to improve protection of the Department information system resources. Security has to be considered throughout the Software Development Life Cycle (SDLC) of an information system. The policy must:

Ensure conformance with all appropriate security requirements.

Protect sensitive and confidential information throughout its life cycle.

Facilitate efficient implementation of security controls.

Prevent introduction of new risks when the system is modified.

Ensure proper removal of data when the system is retired.

3.0 Policy

Appropriate security controls should be considered at all stages of the SDLC including the maintenance stage.

Separate development, testing, and production environments – System development, testing and production should be performed in separate environments.

Test Data – Testing of information systems should be done with fabricated data that mimics the characteristics of the real data, or on copies of real data with any confidential data appropriately sanitized. Testing should not be done on live data due to the threat to its confidentiality and/or integrity. Testing that requires the use of live data or confidential data must have appropriate security controls employed.

Vulnerability Management – An assessment of the system's security controls must be performed on all new enterprise information systems or other systems undergoing significant change before moving them into production. Periodic vulnerability assessments must also be performed on production enterprise information systems and appropriate measures must be taken to address the risks associated with identified vulnerabilities.

Vendor acquisitions – If an information system or component of a system is acquired from an external vendor, written documentation must be provided that specifies how the product meets the security requirements of this policy and any special security requirements of the system. The vendor must allow testing of the system's security controls by the Department or an independent third party, if *needed*.

Change Management – If an information system requires a change once it is in production, the change must be processed through the change control procedures to evaluate the potential impact of change on system security, data integrity and availability. Each change will undergo the same process as new development in testing and verification.

4.0 Terms and Definitions

Information System

An information system and/or server providing services commonly needed by the public or other State Agencies and typically provided by CalHR ITD.

Live Data

Data accessible to users through systems that are in production (i.e. exam information, state applicant information, savings plus information).

Software Development Life Cycle (SDLC)

The process of developing information systems through investigation, analysis, design, implementation and maintenance. It is also known as Information Systems Development of Application Development.

Authority

Government Code Section 11549

State Administrative Manual Section5345

AUTHORITY
State Administrative Manual (SAM) Chapter 5300
California Civil Code 1798 et sequentes
Government Code Section 6250-6270
Government Code Section 8310-8317
Government Code Section 11019.9
Government Code Section 11549
Government Code Section 14613.7(a)
Government Code Section 14740-14741.1
Penal Code 502
Federal Privacy Act of 1974
Federal Information Security Management Act of 2002 (FISMA)

AUTHORIZED USER ACKNOWLEDGEMENT

NAME (Print Full Name) Click here to enter text.	POSITION Click here to enter text.
SUPERVISOR NAME Click here to enter text.	DIVISION Click here to enter text.

Authorized user must read and complete this document, check each item that applies to their position, sign and date, and return it to their immediate supervisor. A copy will be placed in the employee's official personnel file. Employees may periodically be required to update their acknowledgement of these policies.

☐ Acceptable Use

☐ Security Incident Reporting

☐ Clean Desk Policy

☐ Social Media

☐ Access Controls

☐ Malware

☐ Disaster Recovery

☐ Passwords

☐ Software Copyrights

☐ Systems Development and Maintenance

☐ Sensitive and Confidential Information

☐ Portable Computing Devices and Portable Electronic Storage Media

☐ Printer Policy

☐ Physical and Environment

☐ Internet (Web) Monitoring

☐ Network Banner

☐ Password

☐ Risk Management

☐ State Licensed Software on Non-State IT Equipment

☐ Other _____

CERTIFICATION

I certify that I have read and understand all the information contained within the policies checked above. I agree to comply with my responsibilities as an authorized user under all terms of the California Department of Human Resources Information Security Policy (version/date Click here to enter text.). I further certify that non-compliance is punishable as a crime and/ or can result in disciplinary and/or civil action taken against me.

AUTHORIZED USER SIGNATURE	DATE Click here to enter text.

I certify that I reviewed and discussed this Authorized User Acknowledgement with the employee named above.

SUPERVISOR NAME (Print Full Name) Click here to enter text.	SUPERVISOR POSITION Click here to enter text.
SUPERVISOR SIGNATURE	DATE Click here to enter text.

CONFIDENTIALITY STATEMENT

Confidential information is protected from disclosure by law, regulation, and policy. Information security is strictly enforced. If you violate the rules, you may be subject to disciplinary, civil, and/or criminal action. Protecting confidential information is in the public's interest, the state's interest, and your own personal interest.

State employees, student assistants, contractors or volunteers are required to protect the following types of information:

Personal Identifiable Information as described in Civil Code Section1798.30

Recruitment processing activities including testing materials

Methods agencies use to safeguard their information, including computer systems, networks, server configuration, etc.

Information Resources as described in the Information Security Policy Manual

Other agencies' confidential and proprietary information.

State employees, student assistants, contractors or volunteers are required to protect confidential information as follows:

Access, inspect, use, disclose, or modify information only to perform official duties.

Never access, inspect, use, disclose, or modify information, including their own, for curiosity, personal gain, or any non-business related reason.

Never attempt to access, use, disclose, or modify information, including their own, for any non-business or personal reason.

Secure confidential information in approved locations.

Never remove confidential information from work site without prior authorization.

All confidential information must be returned or destroyed 5 days after completion of assignment.

Email or letter confirmation by State employees, student assistants, and contractors must be received by supervisors / managers.

As State employees, student assistants, contractors or volunteers, you are required to know whether information is protected. If you have any questions regarding whether or not information is confidential, check with your department's Information Security Officer.

Communication of Confidential Information – Unless expressly authorized by the Deputy Director, Director, or their designee, authorized users are prohibited from sending, transmitting, or otherwise distributing proprietary, confidential, sensitive, privileged or other state government intellectual property. Confidential information can include internal departmental reports, policies, procedures or attorney-client communications or other internal communications. For example, information related to advice received regarding pending litigation against the employee's agency/department or the Social Security and/or driver's license numbers of members of the public which an employee obtains during the course of his/her duties as a state employee cannot be disseminated. Unauthorized dissemination of such material may result in severe disciplinary action, as well as substantial civil and criminal penalties under State and federal Economic Espionage laws.

Unauthorized access, inspection, use, or disclosure of confidential information is a crime under state and federal laws, including but not limited to: California Penal Code Section 502; California Government Code Section 15619; and California Labor Code Section 1198.6. Unauthorized access, inspection, use, or disclosure may result in any or all of the following:

Administrative discipline, including but not limited to: reprimand, suspension without pay, salary reduction, demotion, and/or dismissal from state service.

Criminal prosecution.

Civil lawsuit.

Termination of contract.

Computer activities may be monitored. Anyone using California Department of Human Resources, State Personnel Board, California Technology Agency, or any other state agency computer systems or any device to access the confidential information consents to such monitoring.

CERTIFICATION

I certify that I understand that information security is strictly enforced and wrongful access, inspection, use, modification, or disclosure or confidential information, or attempts to engage in such acts, is punishable as a crime and/ or can result in disciplinary and/or civil action taken against me. I further certify that I have read the confidentiality statement printed above and have been provided a copy of the Information Security Policy or the location in which to locate it.

NAME (Print Full Name) Click here to enter text.	POSITION Click here to enter text.
SIGNATURE	DATE Click here to enter text.

I certify that I reviewed and discussed this Confidentiality Statement with the employee named above.

SUPERVISOR NAME (Print Full Name) Click here to enter text.	SUPERVISOR POSITION Click here to enter text.
SUPERVISOR SIGNATURE	DATE Click here to enter text.

CONFIDENTIALITY STATEMENT

Confidential information is protected from disclosure by law, regulation, and policy. Information security is strictly enforced. If you violate the rules, you may be subject to disciplinary, civil, and/or criminal action. Protecting confidential information is in the public's interest, the state's interest, and your own personal interest.

State employees, student assistants, contractors or volunteers are required to protect the following types of information:

- Personal Identifiable Information as described in Civil Code Section1798.30
- Recruitment processing activities including testing materials
- Methods agencies use to safeguard their information, including computer systems, networks, server configuration, etc.
- Information Resources as described in the Information Security Policy Manual
- Other agencies' confidential and proprietary information.
- State employees, student assistants, contractors or volunteers are required to protect confidential information as follows:
- Access, inspect, use, disclose, or modify information only to perform official duties.
- Never access, inspect, use, disclose, or modify information, including their own, for curiosity, personal gain, or any non-business related reason.
- Never attempt to access, use, disclose, or modify information, including their own, for any non-business or personal reason.
- Secure confidential information in approved locations.
- Never remove confidential information from work site without prior authorization.
- All confidential information must be returned or destroyed 5 days after completion of assignment.
- Email or letter confirmation by State employees, student assistants, and contractors must be received by supervisors / managers.

As State employees, student assistants, contractors or volunteers, you are required to know whether information is protected. If you have any questions regarding whether or not information is confidential, check with your department's Information Security Officer.

Communication of Confidential Information – Unless expressly authorized by the Deputy Director, Director, or their designee, authorized users are prohibited from sending, transmitting, or otherwise distributing proprietary, confidential, sensitive, privileged or other state government intellectual property. Confidential information can include internal departmental

reports, policies, procedures or attorney-client communications or other internal communications. For example, information related to advice received regarding pending litigation against the employee's agency/department or the Social Security and/or driver's license numbers of members of the public which an employee obtains during the course of his/her duties as a state employee cannot be disseminated. Unauthorized dissemination of such material may result in severe disciplinary action, as well as substantial civil and criminal penalties under State and federal Economic Espionage laws.

Unauthorized access, inspection, use, or disclosure of confidential

information is a crime under state and federal laws, including but not limited to: California Penal Code Section 502; California Government Code Section

15619; and California Labor Code Section 1198.6. Unauthorized access, inspection, use, or disclosure may result in any or all of the following:

- Administrative discipline, including but not limited to: reprimand, suspension without pay, salary reduction, demotion, and/or dismissal from state service.
- Criminal prosecution.
- Civil lawsuit.
- Termination of contract.

Computer activities may be monitored. Anyone using California Department of Human Resources, State Personnel Board, California Technology Agency, or any other state agency computer systems or any device to access the confidential information consents to such monitoring.

CERTIFICATION

I certify that I understand that information security is strictly enforced and wrongful access, inspection, use, modification, or disclosure or confidential information, or attempts to engage in such acts, is punishable as a crime and/ or can result in disciplinary and/or civil action taken against me. I further certify that I have read the confidentiality statement printed above and have been provided a copy of the Information Security Policy or the location in which to locate it.

NAME (Print Full Name)	POSITION
SIGNATURE	DATE

I certify that I reviewed and discussed this Confidentiality Statement with the employee named above.

SUPERVISOR NAME (Print Full Name)	SUPERVISOR POSITION
SUPERVISOR SIGNATURE	DATE

EXHIBIT B
BUDGET DETAIL AND PAYMENT PROVISIONS
INTERAGENCY AGREEMENTS

A. Invoicing

For services satisfactorily rendered and upon receipt and approval of the invoices, the (Agency) agrees to compensate CalHR for actual expenditures incurred in accordance with the services specified on the attached Budget Fee Schedule, Exhibit B-1.

CalHR will submit, in duplicate, an invoice for the total subscription amount contained in Attachment A of this Agreement during the first quarter of the current fiscal year. All invoices will include the Agreement Number and will be submitted in duplicate and not more frequently than monthly, in arrears, to:

(Agency)
(Attn)
(Address)

B. Budget Contingency Clause

1. It is mutually agreed that if the Budget Act of the current year and/or any subsequent years covered under this Agreement does not appropriate sufficient funds for the program, this Agreement shall be of no further force and effect. In this event, the State shall have no liability to pay any funds whatsoever to Contractor or to furnish any other considerations under this Agreement and Contractor shall not be obligated to perform any provisions of this Agreement.

2. If funding for any fiscal year is reduced or deleted by the Budget Act for purposes of this program, the State shall have the option to either cancel this Agreement with no liability occurring to the State, or offer an agreement amendment to Contractor to reflect the reduced amount.

3. Contractor reserves the right to ask for an amendment in the event there is an increase in costs in the current year and/or any subsequent years covered under this Agreement.

C. Payment

1. Costs for this Agreement shall be computed in accordance with State Administrative Manual Sections 8752 and 8752.1.

2. Nothing herein contained shall preclude advance payments pursuant to Article 1, Chapter 3, Part 1, Division 3, Title 2 of the Government Code of the State of California.

D. Non-Payment

If payment has not been received for a non-disputed invoice within 60 days of the invoice date, CalHR, in accordance with Government Code Section 11255, will provide the agency with a 30-day notification of its intent to initiate a Transaction Request with the State Controller's Office to transfer funds from the agency to CalHR.

The agency will provide the following appropriation data to the CalHR:

Fund Number:	
Organization Code:	
Fiscal Year:	
Reference:	
Category or Program:	
If applicable, the agency will additionally provide the Element, Component and Task:	

EXHIBIT B, ATTACHMENT 1
FEE SCHEDULE

DESCRIPTION	FREQUENCY	FEE AMOUNT
401(k) Pre-Tax Deductions	N/A	No Fee ($0)
401(k) Designated Roth Deductions	N/A	No Fee ($0)
401(k) Loan Deductions	N/A	No Fee ($0)
457 Pre-Tax Deductions	N/A	No Fee ($0)
457 Designated Roth Deductions	N/A	No Fee ($0)
457 Loan Deductions	N/A	No Fee ($0)
Alternate Retirement Program (ARP) Deductions	Per Deduction	$4.80
Part-time, Seasonal, and Temporary (PST) Deductions	Per Deduction	$2.45
Delinquent File	Per Account	$500.00
Failure to Report	Per File	$50.00
Administrative Delinquency	Per Processing Period	$25.00
CalHR IT Support	Per Infraction <u>Example:</u> 1. File Name Error 2. Header/Footer/Trailer Error 3. Duplicate File Error 4. Delinquent Upload Error	$50.00

EXHIBIT C
GENERAL INTERAGENCY AGREEMENT TERMS AND CONDITIONS (GIA 610)

1. APPROVAL: This Agreement is not valid until signed by both parties and approved by the Department of General Services, if required.

2. AUDIT: The agency performing work under this Agreement agrees that the awarding department, the Department of General Services, the Bureau of State Audits, or their designated representative shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement if it exceeds ten thousand dollars ($10,000). The agency performing work agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of record retention is stipulated.

3. PAYMENT: Costs for this Agreement shall be computed in accordance with State Administrative Manual Section 8752 and 8752.1.

4. AMENDMENT: No amendment or variation of the terms of this Agreement shall be valid unless made in writing, signed by the parties, and approved as required. No oral understanding or agreement not incorporated in the Agreement is binding on any of the parties.

5. SUBCONTRACTING: All subcontracting must comply with the requirements of the State Contracting Manual, Section 3.06.

6. ADVANCE PAYMENT: The parties to this interagency agreement may agree to the advancing of funds as provided in Government Code Sections 11257 through 11263.

7. DISPUTES: The agency performing work under this Agreement shall continue with the responsibilities under this Agreement during any dispute.

8. TIMELINESS: Time is of the essence in this Agreement.

9. NON-PAYMENT OF INVOICES – FUND TRANSACTION REQUEST: In accordance with Government Code Section 11255, the parties agree that when an invoice is not paid by the requested due date to the Contractor (agency providing the service) and the invoice is not disputed by the contracting Department (agency receiving the service), Contractor may send the contracting Department a thirty (30) day notice that it intends to initiate a transfer of funds through a Transaction Request sent to the State Controller's Office. To facilitate a Transaction Request should one be needed, the contracting Department shall no later than ten (10) business days following execution of this agreement provide data to the Contractor for the appropriation to be charged including: fund number, organization code, fiscal year, reference, category or program, and, if applicable, element, component, and task.

EXHIBIT D –
SPECIAL TERMS AND CONDITIONS FOR DEPARTMENT OF HUMAN RESOURCES
(INTERAGENCY AGREEMENTS)

A. TERMINATION CLAUSE: Either State agency may terminate this Agreement upon thirty (30) days' advance written notice. The State agency providing the services shall be reimbursed for all reasonable expenses incurred up to the date of termination.

B. SEVERABILITY: If any provision of this Agreement is held invalid or unenforceable by any court of final jurisdiction, it is the intent of the parties that all other provisions of this Agreement be constructed to remain fully valid, enforceable, and binding on the parties.

C. CONFLICT OF INTEREST:

1. Current and Former State Employees: Contractor should be aware of the following provisions regarding current or former state employees. If Contractor has any questions on the status of any person rendering services or involved with the Agreement, the awarding agency must be contacted immediately for clarification.

   a) Current State Employees: (PCC §10410)

      1) No officer or employee shall engage in any employment, activity or enterprise from which the officer or employee receives compensation or has a financial interest and which is sponsored or funded by any state agency, unless the employment, activity or enterprise is required as a condition of regular state employment.

      2) No officer or employee shall contract on his or her own behalf as an independent contractor with any state agency to provide goods or services.

   b) Former State Employees: (PCC §10411)

      1) For the two-year period from the date he or she left state employment, no former state officer or employee may enter into a contract in which he or she engaged in any of the negotiations, transactions, planning, arrangements or any part of the decision-making process relevant to the contract while employed in any capacity by any state agency.

      2) For the twelve-month period from the date he or she left state employment, no former state officer or employee may enter into a contract with any state agency if he or she was employed by that state agency in a policy-making position in the same general subject area as the proposed contract within the 12-month period prior to his or her leaving state service.

   c) Penalty for Violation:

      1) If the Contractor violates any provisions of above paragraphs, such action by Contractor shall render this Agreement void. (PCC §10420)

   d) Members of Boards and Commissions:

      1) Members of boards and commissions are exempt from this section if they do not receive payment other than payment of each meeting of the board or commission, payment for preparatory time and payment for per diem. (PCC §10430 (e))

e) Financial Interest in Contracts:
Contractor should also be aware of the following provisions of Government Code §1090:
"Members of the Legislature, state, county district, judicial district, and city officers or employees shall not be financially interested in any contract made by them in their official capacity, or by any body or board of which they are members. Nor shall state, county, district, judicial district, and city officers or employees be purchasers at any sale or vendors at any purchase made by them in their official capacity."

D. ORDER OF PRECEDENCE:

In the event of any inconsistency between the terms, specifications, provisions or attachments which constitute this Contract, the following order of precedence shall apply:

1. The General Terms and Conditions for Interagency Agreements;
2. The Std. 213;
3. The Scope of Work;
4. Any other incorporated attachments in the Contract by reference